



## User Guide

August 2021 | Version 10.4

This page intentionally left blank.

## Preface

This user guide addresses only the most recent version of Inspector.

## Legal Information

Copyright © 2021 Cellebrite DI Ltd. All rights reserved.

This publication is expressly subject to the Cellebrite DI Ltd. ("Cellebrite") End User License Agreement and other applicable terms and condition of sale and license and is further subject to the terms, conditions, and restrictions described herein. This publication contains proprietary and confidential information owned by Cellebrite. This publication is solely for use by authorized Cellebrite customers exclusively for use with Cellebrite products. This publication may not be disclosed to any person or firm, or reproduced by any means, electronic or mechanical, in whole or in part, without the express prior written permission of Cellebrite. The text and graphics contained herein are for the purposes of illustration and reference only. Cellebrite reserves the right to revise this publication at any time without notice. The specifications on which this publication is based are subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

Cellebrite®, CELLEBRITE DIGITAL INTELLIGENCE FOR A SAFER WORLD®, CCME®, and BLACKBAG A CELLEBRITE COMPANY™ are registered and unregistered trademarks of Cellebrite DI Ltd.

All other brand and product names are trademarks or registered trademarks of their respective holders.

## Typographic Conventions

This document uses these typographic conventions.

- The names of windows, views, tabs, dialog boxes, panes, panels, buttons, fields, options, checkboxes, and the like are in Initial Caps, or otherwise capitalized according to their labels.
- Keystrokes are shown in all capital letters, such as TAB, CTRL, OPT, CMD, SPACEBAR. Keys pressed at the same time are joined with +, such as CTRL+S, OPT+T.
- The names of elements that you are directed to interact with by clicking, selecting, or typing are shown in **bold**.
- Immediately contiguous menu actions such as clicking a toolbar button or menu, then immediately clicking another item in a resulting submenu, are separated with the > symbol, such as

**Edit > Copy**

**Preferences > Data Collection**

- *File names, folder names, file paths, disk names, drive names, volume names, partition names, and the like are shown in italic.* File extensions such as .pdf, .docx., .jpg, and so forth are not shown in italic.
- Variables are enclosed with <angle brackets>, such as <PLATFORM> VOLUMES, where <PLATFORM> is either MACOS or WINDOWS.
- **Anything you are directed to type exactly, such as file names, commands, or code, are shown in a console font.**

If you find any typos, inaccuracies, or other problems in this documentation, please send an email to [support@cellebrite.com](mailto:support@cellebrite.com). Please include the title of the document, the version of the document, and the title of the topic in your message.



## Contents

<b>Document Revision History.....</b>	<b>1</b>
Inspector Version 10.4 .....	1
<b>What's New in Version 10.4.....</b>	<b>2</b>
Classification .....	3
Define Classifications .....	3
Classify Items .....	3
See Classified Items .....	4
Filter by Classification .....	4
Remove Classifications from Items .....	4
Apply and Remove Classifications with Tags .....	5
Classifications in Portable Cases .....	5
Activity Correlation.....	6
Expanded Support for Dictionary Attacks.....	6
Internet Domain Categories .....	8
Usability Improvements.....	9
Improved Support for macOS Big Sur .....	9
Imaging and Evidence Ingestion .....	9
Indexing Performance .....	11
Hex View Highlight .....	11
Support for License Management .....	12
Censored Pictures and Videos .....	13
Filtering .....	13
<b>Introduction.....</b>	<b>14</b>
Intended Audience .....	14
Digital Forensics Overview .....	15
Preserving and Acquiring Digital Forensic Evidence.....	15
Hardware and Software Requirements .....	18
Recommended Hardware Requirements.....	18
Minimum Hardware Requirements .....	18
Minimum Software Requirements.....	19
Installing Inspector .....	19
Registration .....	19
Analyzing Digital Evidence.....	20
Hashing Individual Files.....	20

Known File Hash Set Database .....	20
Searching.....	20
Tagging .....	21
Reporting .....	21
Generating Reports.....	21
Sharing Cases .....	21
Backing Up Case Evidence .....	21
Getting Support .....	22
<b>Workspace Orientation.....</b>	<b>23</b>
Case Manager Window .....	23
Case Info View .....	24
Case Window .....	25
Toolbar.....	26
Component List.....	27
File Information Pane .....	28
Content Pane.....	29
View Filter.....	29
File Content View .....	30
The Status Bar.....	32
Menu Bar .....	32
Inspector Menu .....	33
File Menu.....	35
Edit Menu.....	38
Action Menu.....	38
Tags Menu .....	46
View Menu .....	47
Manage Menu.....	48
Window Menu .....	48
Help Menu .....	49
Toolbar.....	49
Component List.....	52
Evidence.....	53
Activity.....	55
Content Searches.....	58
Index Searches.....	58
Tags.....	58
Investigative Notes.....	59
Details View .....	60

Details View for Disk Images.....	60
Details View for Partitions and Imported Folders.....	61
Details View for Mobile Devices .....	64
Details View for Other Types of Evidence Items.....	65
File Information Pane .....	66
File System and Operating System Unique Metadata .....	67
Media File Metadata.....	67
File Content View .....	68
Hex .....	69
Strings .....	70
Preview .....	70
Metadata.....	72
Record .....	73
Data Interpreter View.....	74
Hex Templates and Data Structure View.....	75
Recovered SQLite Records.....	83
Viewing Embedded .plist Data and .jpg Pictures.....	84
Managing List Views .....	85
Column Reordering.....	85
Settings, Preferences, and Options .....	87
Inspector Preferences or Options.....	87
System Preferences on Mac Computers.....	97
System Settings on Windows 10 Computers.....	99
<b>Managing Case Evidence .....</b>	<b>101</b>
Create a New Case .....	101
Inspector Time Zone Settings .....	102
Open a Case.....	103
Update a Case to Work in a Newer Version of Inspector.....	103
Adding Evidence to a Case.....	104
Supported File Systems.....	106
Add Evidence Items.....	106
Adding a Disk Image .....	111
Adding a Selected Image File on an Imported Evidence Item.....	120
Adding an iOS Disk Image or Backup .....	120
Ingest GrayKey Images .....	123
Adding a Memory File .....	125

Adding a USB Attached Mobile Device.....	128
Adding Other Attached Devices.....	130
Adding a Mobilyze Case .....	130
Adding a Folder or File .....	131
Adding Evidence Using Drag and Drop.....	131
Adding Berla iVe.....	132
Adding iCloud Productions .....	133
Adding UFED and Premium CAIS Acquisitions .....	137
Remove Evidence from a Case.....	137
Move a Case File to a Different Computer .....	138
Relocating a Disk Image.....	138
Exporting Mobile Device Evidence .....	139
Hashing and Verifying Forensic Evidence.....	139
Advanced Evidence Recovery .....	140
Manually Setting Disk Sector Size .....	141
Editing a Partition .....	141
Defining a Deleted or Missing Partition.....	141
Importing or Processing a Drive or Partition as Unallocated Space .....	142
Creating an .iso Disk Image from a Partition.....	142
File Entropy .....	143
<b>Timeline View .....</b>	<b>145</b>
Time Scale .....	145
Artifacts in Timeline.....	146
Timeline Details .....	147
Additional Timeline Features .....	148
<b>Browser View .....</b>	<b>149</b>
Working with Columns.....	150
Type-Down in List Views.....	151
Special Fonts and Icons in Browser View.....	151
Volume Shadow Copies .....	152
<b>File Filters.....</b>	<b>154</b>
Individual File Filter Options.....	157
List All Files.....	158
Name .....	158
Path.....	159
Kind.....	159
Extension .....	161
Content Extension.....	161
Extension Matching.....	162

Tagged State.....	162
Tag Name .....	162
Size.....	162
Owner.....	163
Group .....	163
Permission .....	163
Dates Created, Modified, Accessed, and Added.....	164
BL ID .....	164
File System ID .....	165
Hash Set .....	165
Hash Set Category .....	166
File Hash.....	166
List Duplicate Files .....	166
File Entropy .....	166
Soft Link Path.....	167
Hard Link Target ID .....	167
Directory .....	167
Locked .....	167
Resource Fork.....	168
Alternate Data Stream.....	168
Visibility.....	168
iOS Hidden Item .....	168
Metadata Field.....	169
Metadata Value.....	169
Metadata Field Value .....	169
Spotlight Field .....	170
Spotlight Value .....	170
Spotlight Field Value .....	170
Internal Filter .....	170
Snapshot (APFS) / Volume Shadow Copy (NTFS).....	171
OCR Image Text.....	171
Using File Filters.....	172
Saving and Managing File Filters.....	172
Applying a Preset Filter or Saved File Filter .....	172
Filtering within Specific Views.....	173
Locating Live Victims .....	174
Locating Picture or Video Files Created at the Same Location .....	175
Sorting Media Files by Calculated Skin Percentage .....	178
Sorting Media Files by Image Analyzer Categories .....	178
Mapping GPS Metadata Using Google Maps .....	179
Mapping GPS Metadata Using Google Earth.....	179
Search .....	180

Content Keyword Searches .....	180
Adding Keywords to Content Searches.....	183
Regular Expression Presets.....	183
Saved Content Search Settings.....	186
Applying Filters to a Content Search .....	186
Filtering Search Results .....	187
Viewing Content Search Results and Criteria .....	187
Criteria Tab.....	188
Statistics Tab .....	189
Index Searching.....	189
Creating a Smart Index Query .....	189
Bulk Extraction Searches on Memory Files .....	192
<b>Media View .....</b>	<b>194</b>
Analyzing Picture and Video Files .....	194
Sticky Select .....	195
Thumbnails.....	195
Geolocation Metadata .....	197
Export Location Data as KMZ or KML.....	197
Image Categorization with Image Analyzer .....	198
Analyzing Audio Files .....	201
<b>Communication View.....</b>	<b>202</b>
Phone Artifacts.....	202
Calls .....	202
Voicemail .....	203
Voice Memos .....	204
Favorites .....	204
Messaging .....	204
Social Media .....	206
Contacts.....	208
Email.....	209
Support for EMLX and EMLX Partial.....	211
<b>Locations, Internet, and Productivity Views .....</b>	<b>213</b>
Locations View.....	213

Map View Sub-view .....	213
Location List Sub-view.....	215
Wi-Fi Sub-view .....	217
Internet View .....	218
Productivity View .....	219
Calendar Sub-view.....	219
Notes Sub-view .....	220
<b>System View .....</b>	<b>221</b>
Registry.....	221
Shellbags .....	223
Spotlight .....	224
Tagging Spotlight Data .....	226
Dictionary.....	227
Applications .....	227
System Logs .....	228
File System Logs.....	228
Unified Logs.....	229
Memory.....	230
<b>Actionable Intel View.....</b>	<b>231</b>
Device Backups.....	231
Exporting iOS Backups .....	231
Importing iOS Backups .....	232
Device Connections.....	233
Account Usage .....	233
Cellular Usage.....	233
Top Contacts.....	234
User Accounts .....	234
Downloads .....	235
AirDrop .....	235
Files .....	236
File Knowledge.....	237
Link Files .....	237
Recent Items .....	237

Trash Items .....	240
Passwords .....	241
Viewing Keychain Data.....	243
Tagging and Reporting Keychain Data.....	243
Program Execution .....	244
Search.....	246
Activity Correlation.....	247
<b>Plugins View .....</b>	<b>250</b>
APOLLO Plugin.....	250
Get a new version of the APOLLO Plugin.....	251
Use the APOLLO Plugin.....	251
<b>Tags.....</b>	<b>252</b>
Adding Tags .....	252
Configure Metadata for Tags.....	253
Tagging Evidence .....	254
Tagging File Content.....	255
Tagging Email.....	255
Tagging External Content .....	256
Tags View .....	257
Deleting Tags .....	259
<b>Reporting.....</b>	<b>260</b>
Report View .....	260
Tags and Tagged Items.....	261
Reporting Device Details .....	262
Generating and Exporting the Examiner Report .....	263
<b>Portable Cases.....</b>	<b>264</b>
Select Data for the Portable Case .....	264
Extracted Data.....	265
Tags.....	266
Search.....	266
Generating and Reviewing a Portable Case .....	267
Reviewing a Portable Case .....	267
Portable Case Interface.....	268



Menu Bar .....	268
Toolbar .....	269
Component List .....	270
Content Pane .....	272
File Content View .....	273
Accessing Portable Case Files .....	274
<b>Hash Set and File Signature DB Management .....</b>	<b>275</b>
Hash Sets .....	275
File Signature Databases .....	278
PhotoDNA and Project VIC .....	279
Add the Project VIC Robust Hash Set to Inspector .....	279
C4All .....	280
Semantics21 .....	282
Export Images and Videos .....	282
Connect Inspector to the S21 SQL Database .....	283
<b>File System Information .....</b>	<b>284</b>
Apple File System .....	284
Adding APFS Evidence to Inspector .....	285
APFS Snapshot Parsing .....	286
APFS on macOS 10.15 .....	288
Artifact Items .....	291
Spotlight Index .....	291
NTFS Access Control Lists .....	292
Cocoa Nanosecond Timestamp Format .....	293
<b>Troubleshooting .....</b>	<b>294</b>
The Debug Console .....	294
Enable Verbose Mode .....	294
Other Issues .....	296
Exception Errors .....	296
Database Errors .....	296
Locating Partitions .....	297
<b>Appendix 1 - iTunes Precautions .....</b>	<b>298</b>
Disable iTunes on a Mac Computer .....	298
Permanently Disable iTunesHelper on a Mac Computer .....	299

Temporarily Disable iTunesHelper on a Mac Computer .....	299
Disable Auto-Launch of Camera-Related Applications on Mac Computers.....	300
Disable iTunes on a Windows 10 Computer .....	300
Disabling Windows AutoPlay features .....	301
<b>Appendix 2 - EWMounter.....</b>	<b>302</b>
Mounting Options .....	303
Verifying MD5 and SHA1 Hash Values .....	305
Previewing a Mounted E01 Image File.....	306
Previewing in Finder .....	306
Previewing in Inspector .....	307
Shadow Mounting an E01 Image File.....	307
Unmounting an E01 Image File.....	309
Extracting RAW images from EWMounter .....	310
<b>Appendix 3 - Inspector License Server Configuration .....</b>	<b>311</b>

## Document Revision History

This user guide addresses only the most recent version of Inspector.

This topic identifies information that is new, removed, or changed within this document in this version of Inspector.

### Inspector Version 10.4

Description	Topic
This topic is new.	Document Revision History
Moved this topic from the Preface to the <a href="#">Introduction</a> .	<a href="#">Intended Audience</a>
This chapter is new.	<a href="#">What's New in Version 10.4</a>
Improved information about ensuring email previews is available in reports.	<ul style="list-style-type: none"><li>• <a href="#">Inspector Preferences or Options</a>: In the Report Tab section, revised the last sentence and its note.</li><li>• <a href="#">Email</a>: Added sentence before numbered steps.</li><li>• <a href="#">Tagging Evidence</a>: Added the section titled Tagging Email.</li><li>• <a href="#">Generating and Exporting the Examiner Report</a>: Added paragraph about including email previews in reports.</li></ul>
Added information to setting maximum number of processors Inspector should utilize.	<a href="#">Inspector Preferences or Options</a> : In the Options Tab section, added the last two sentences to the first paragraph under Processing Options.
Deleted this topic: Creating and Opening a Case	The information is now in two distinct topics. <ul style="list-style-type: none"><li>• <a href="#">Create a New Case</a></li><li>• <a href="#">Open a Case</a></li></ul>

## What's New in Version 10.4

This chapter presents information about features that are new or changed in version 10.4 of Inspector.

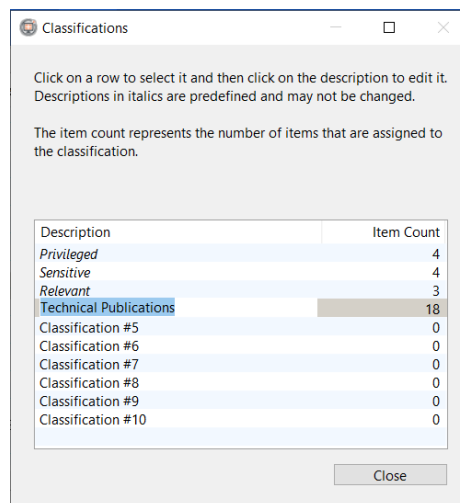
- [Classification](#)
  - [Define Classifications](#)
  - [Classify Items](#)
  - [See Classified Items](#)
  - [Filter by Classification](#)
  - [Remove Classifications from Items](#)
  - [Apply and Remove Classifications with Tags](#)
  - [Classifications in Portable Cases](#)
- [Activity Correlation](#)
- [Expanded Support for Dictionary Attacks](#)
- [Categorize Internet Domains](#)
- [Usability Improvements](#)
  - [Improved Support for macOS Big Sur](#)
  - [Imaging and Evidence Ingestion](#)
    - [Image Attached Drives](#)
    - [Ingest Backups from Within Images](#)
    - [Ingest .UFD Files](#)
    - [Windows Search Index and Metadata](#)
  - [Indexing Performance](#)
  - [Hex View Highlight](#)
  - [Support for License Management](#)
  - [Censored Pictures and Videos](#)
  - [Filtering](#)

## Classification

The new classification feature provides another facet for identifying evidence items and managing how they are seen in portable cases and reports. The first three classifications, Privileged, Sensitive, and Relevant, cannot be edited. You can define the remaining seven classifications as necessary.

### Define Classifications

1. Open or create a case file and then click **Manage > Classifications**.  
The Classifications dialog box appears.
2. Select any classification other than Privileged, Sensitive, or Relevant.
3. For the selected classification, click in the **Description** column.



4. Type the appropriate name for this classification and then press ENTER.

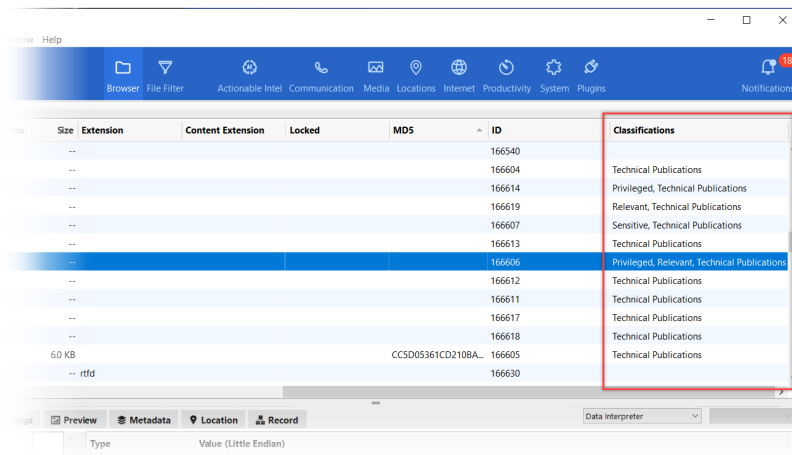
### Classify Items

You can classify evidence items in all views individually or with several items selected at once. You can apply more than one classification.

- Select the item, click **Classifications > Classify Files As**, and then select the appropriate classification.
- Select the item, open the context menu, click **Classifications > Classify Files As**, and then select the appropriate classification.

## See Classified Items

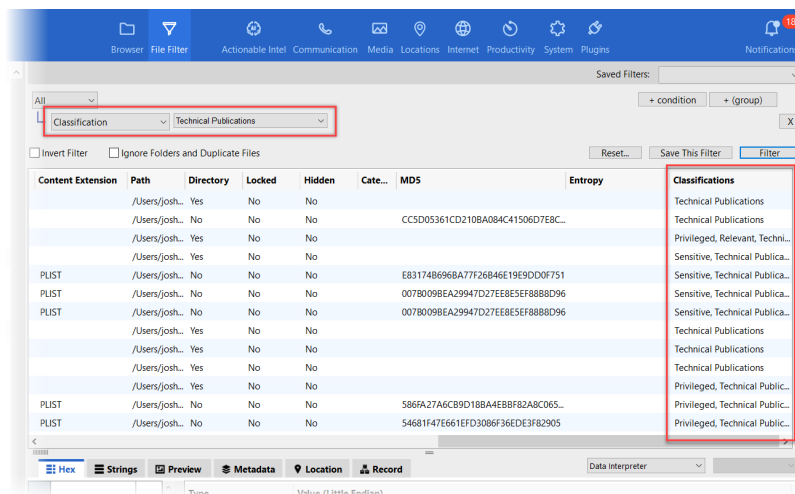
The Classification column is available in all views as the last column. You can sort this column.



Multiple classifications are separated by commas and the order is always the same as the list of classifications.

## Filter by Classification

Classification is available in the File Filter view and when filtering within specific views.



## Remove Classifications from Items

You can remove all or any single classification from items.

- Select the item, click **Classifications > Remove Classification from Files**, and then select either the appropriate classification or select **All**.
- Select the item, open the context menu, click **Classifications > Remove Classification from Files**, and then select either the appropriate classification or select **All**.

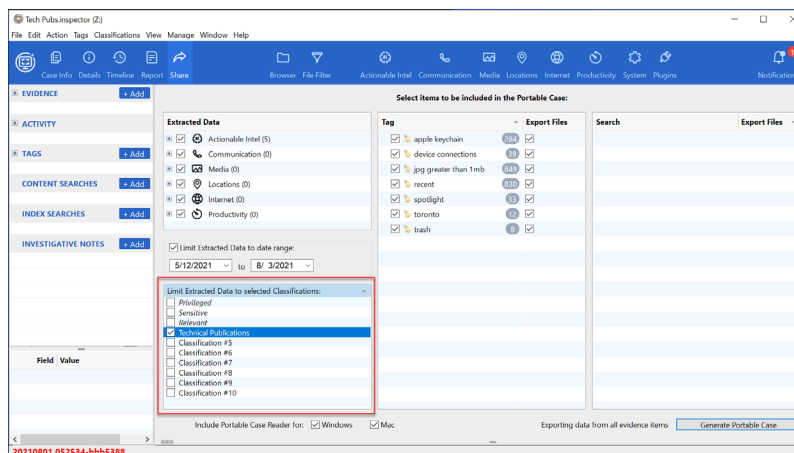
## Apply and Remove Classifications with Tags

You can use tags as a means to apply classifications to items and remove classifications from items.

1. Under TAGS in the Component list, click the appropriate tag.
2. To apply a classification to all items with this tag, open the context menu, click **Classify Tagged Items As**, and then click the appropriate tag.
3. To remove a classification from all items with this tag, open the context menu, click **Remove Classification from Tagged Items**, and then click the appropriate tag or click **All**.

## Classifications in Portable Cases

When you create a portable case, you can limit extracted data with classifications. If you select any classifications, only data with the selected classifications appears in the portable case, as well as data with no classifications. Data with different (not selected) classifications does not appear in the portable case.



For example, consider a case using the three pre-defined classifications, Privileged, Sensitive, and Relevant. Some data is only classified once, some twice, and some with all three classifications. When you create a portable case, you choose to include only data classified as Sensitive and Relevant; you do not select Privileged. In the portable case, this is the result.

- Data classified only as Privileged does not appear.
- Data classified as either or both Sensitive and Relevant does appear.
- Data classified as Privileged and also either Sensitive or Relevant does appear.
- Data classified with all three classifications does appear.

## Activity Correlation

In the Actionable Intel view, activity correlation now supports images from Mac computers. The Correlation view also now supports filtering, and in particular lets you filter on date and time. This provides a time-based view that shows how an artifact came to be and how it is related to other artifacts. For more information, see [Filtering](#).

These usability enhancements were made to the Correlation view.

- Splitters have been added to let you change the size of all the panes.
- When an item in the middle pane has very long text in a column, you can now hover your mouse pointer over that text to see all of it, rather than scrolling and resizing columns.
- These filters have been added: Owner, Event Type, Description, and Artifact Count.

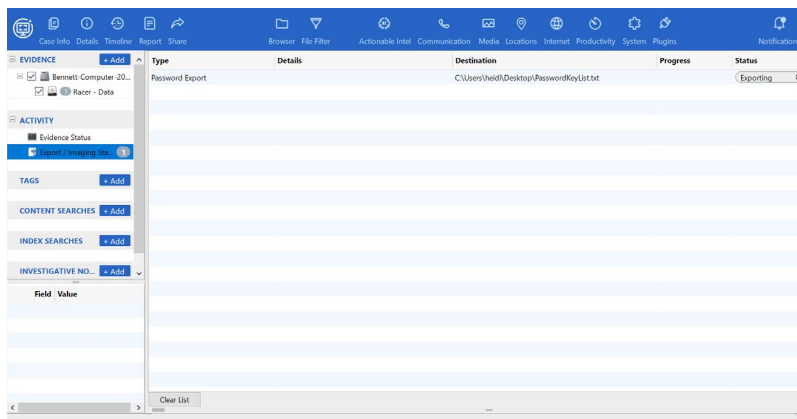
## Expanded Support for Dictionary Attacks

Inspector has expanded support for creating custom dictionary files with password candidates for use in investigations. This support is in the form of an exported .TXT file with one word on each line, without duplicates. This .TXT file provides key material for use by third-party software, such as Passware Kit Forensic.

For both Windows and Mac images, you can extract the index.

**Note:** This process can take some time to complete.

1. Run indexing in Inspector for the appropriate volumes.
2. When indexing is complete, select the volumes to export.
3. Click **Action > Export > Export Password Key List**.
4. Specify the destination and filename for the exported .txt file.
5. To see progress, in the Component list click **Export / Imaging Status** under Activity.



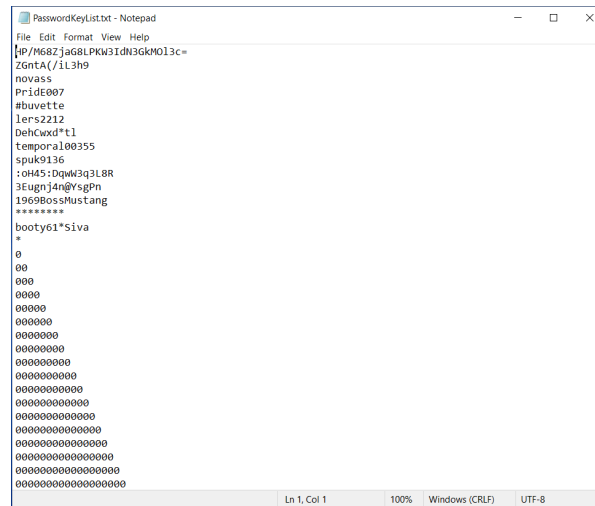
For the password export in progress, you can see the destination you specified, the duration of the export, and the status.



- During export, you can pause or delete the action.
  - To pause an export in progress, click **Exporting** and then click **Pause**. To resume a paused export, click **Paused** and then click **Resume**.
  - To delete the export in progress, click **Exporting** and then click **Delete Item**.

When the export is complete, the status becomes Finished.

You can find the exported .TXT file in the destination you specified. This is an example.

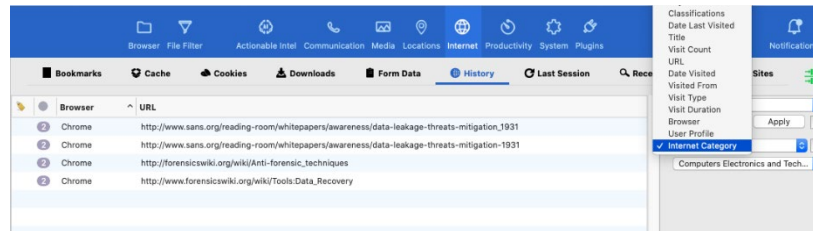


**Note:** It may take some time to open the .TXT file if it is very large.

For images ingested from Mac OSX 10.x through Mojave 10.14.3 and from iOS 9.x through 12.x, Inspector can also export password hashes, custom dictionary entries, and keychain files.

## Internet Domain Categories

Internet domains are now automatically categorized according to a list created by Cellebrite. Accordingly, Internet Category is a new filter option for the Internet views.



The list of categories is determined by the nature of the domains for internet artifacts ingested for the entire case. It can include a wide variety of categories in broad areas such as arts and entertainment, business and consumer, computers, electronics and technology, hobbies and leisure, and many more.

Internet domains that include sites with risk for malware and cryptocurrency, for example, appear in categories like these.

- "Computers Electronics and Technology/Computer Security" for Bitcoin and malware
- "Finance/Finance" for Dogecoin

## Usability Improvements

Improvements and usability enhancements were made in these areas.

- [Improved Support for macOS Big Sur](#)
- [Imaging and Evidence Ingestion](#)
- [Indexing Performance](#)
- [Hex View Highlight](#)
- [Support for License Management](#)
- [Censored Pictures and Videos](#)
- [Filtering](#)

### Improved Support for macOS Big Sur

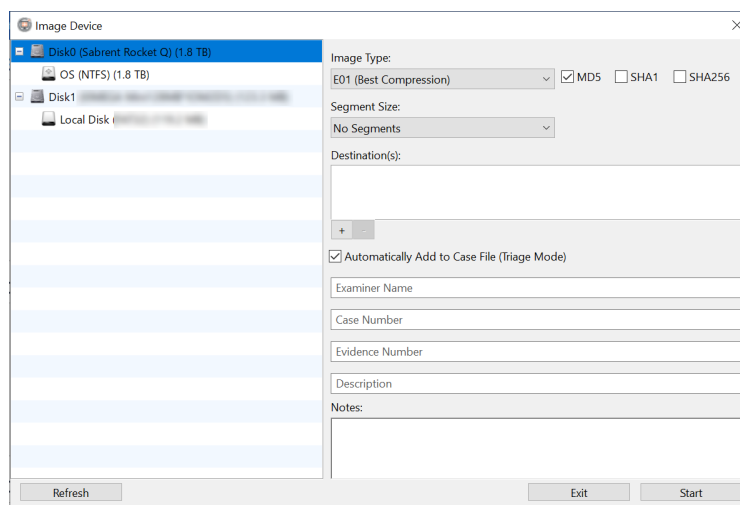
For macOS 11 Big Sur, system partitions can now be ingested and parsed. Spotlight, Bluetooth, and Wi-Fi are also now supported.

### Imaging and Evidence Ingestion

There are several enhancements for imaging and evidence ingestion.

#### Image Attached Drives

Inspector can now acquire full disk or logical images of attached drives. These attached drives must be write-blocked either with software- or hardware-based write blockers. With the drive connected, click **Action > Disk Imaging**.



The Image Device dialog box shows only the options appropriate for the selected image type. To save time when triaging, you can use the **Automatically Add to Case File (Triage Mode)** checkbox to set whether to ingest after imaging. You can see information about ingestion and processing when you select **Export / Imaging Status** under Activity in the Component list.

## Ingest Backups from Within Images

Inspector can now directly ingest device backups from within images, rather than exporting and ingesting the backup into the case file. This improves efficiency and reduces the size of case files. These file types may be imported from **Actionable Intel > Insights > Device Backups**.

- .E01
- iPhone backups
- plain files and directories
- raw disk images
- some specific .dmg types
- .zip
- .tar

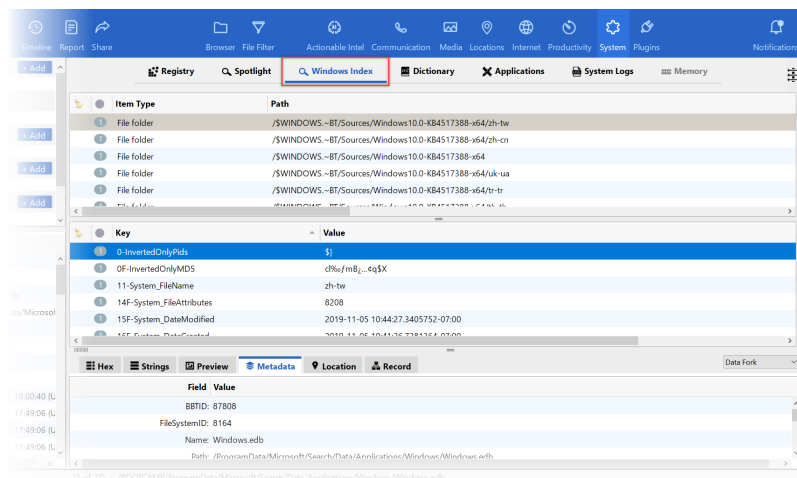
If .zip or .tar files are imported and Process Archives is selected, they appear as an evidence source with all the contents of the archive in the file browser for that evidence source.

## Ingest .UFD Files

On the Add Evidence window, you can now select .UFD files (not .UFDX files) from any collection and the corresponding compressed evidence files are automatically selected and ingested. The collection must be in its original unaltered folder structure. If you prefer, you can still manually select compressed files instead, such as .TAR, .ZIP, and .DAR.

## Windows Search Index and Metadata

On the Add Evidence window, when you select Actionable Intel for the Extract Data processing option, data is automatically parsed from the Windows search index and file metadata is added to the associated files after processing. You can see the result on the new Windows Index view in System view, where keys and values appear for each selected item type. If Windows metadata is available for a selected file, you can see it in the Windows Metadata section in the Metadata view.



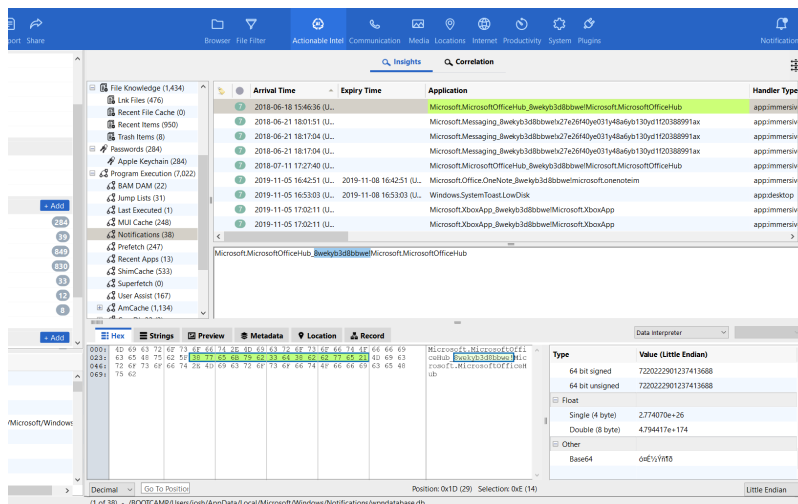
## Indexing Performance

Inspector now uses SQLite instead of Elastic Search for Index searching. Within Inspector, the Help topic for the Query Name field in Index Search has been updated accordingly. For more information, see this page: [https://sqlite.org/fts5.html#full\\_text\\_query\\_syntax](https://sqlite.org/fts5.html#full_text_query_syntax).

Indexing now runs faster than before, and Inspector is more responsive now during indexing. Indexing still takes longer to complete than other processing options. Run the index process only when it is necessary, and with the expectation that it will take time to complete.

## Hex View Highlight

For certain item types in the Insights view under Actionable Intel, when you select part of a file's content in the lower portion of the Content pane, the corresponding content is also highlighted in Hex view. It also appears in the related Data Interpreter view as a String.



This is available for these items in Actionable Intel > Insights.

- Passwords > Apple Keychain
- Program Execution > Notifications
- All items in ComDlg32
- All items in Windows Activity Timeline

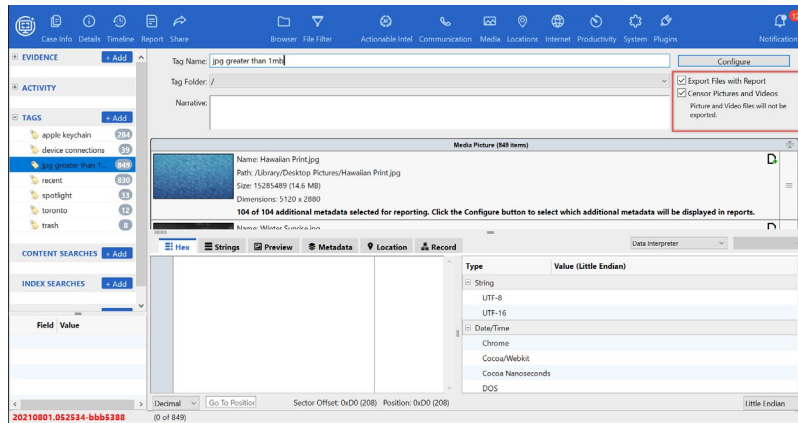
## Support for License Management

The License Manager application is no longer required for managing Inspector licenses. Now, you can update your license file directly from within Inspector. The options on the Help menu have been changed to support this. This is the Help menu now.

Option	Description
Cellebrite Website	Open the Cellebrite home page in a web browser
Inspector Feedback	Send an email to Cellebrite to provide feedback about Inspector
Technical Support	Open the technical support page on the Cellebrite website in a web browser
Update Dongle License	Open the Update Dongle window, where you find and select the license file for your Inspector device and click <b>Update</b> . The license filename uses this pattern: <i>bdtlicense_&lt;serialNumber&gt;</i> , where <i>&lt;serialNumber&gt;</i> is the serial number for your Inspector device.
Enter License Key	Used for demonstration purposes with cooperation from Cellebrite sales. If an Inspector device (dongle) is connected to the computer, this option does not open the window.
About Inspector (Only on Windows)	Open the About Inspector window, which shows the version, build, dongle ID (serial number), and expiration for Inspector as well as contact information.
Check for Updates (Only on Windows)	Check for a newer version of Inspector

## Censored Pictures and Videos

When you select a picture type tag, you can now set whether censored pictures and videos are exported with reports. Also, the user interface when configuring a tag makes it more clear that choosing to censor photos affects both photos and videos.



## Filtering

For all views except the File Filter view, filtering based on time now includes hours and minutes in addition to date.

These more robust time-based options have been added.

- is exactly (with HH:MM)
- is after (with HH:MM)
- is before (with HH:MM)
- is between (with HH:MM)
- is not (with HH:MM)

## Introduction

Inspector is a comprehensive software solution to help investigators conduct digital forensic investigations on Mac computers, iOS devices (iPhone, iPad, iPod touch), Android devices, and Windows computers. Inspector is designed for both novice and advanced users and offers a clean interface featuring easy navigation as well as powerful advanced options. The interface provides forensic examiners both robust capabilities and an intuitive and elegant user experience throughout all phases of a digital forensic investigation.

With Inspector, you can accomplish these tasks.

- Manage cases.
- Collect files from remote computers (only for customers using Endpoint Inspector, offered by Cellebrite Enterprise Services.)
- Ingest, manage, and verify evidence.
- Browse, search and filter evidence.
- Analyze evidence with views focused on timelines, media, communications, locations, internet activity, productivity tools, system activities, and actionable intelligence.
- Tag evidence, create reports, and share evidence in portable case files.

This chapter provides these topics about Inspector.

- [Intended Audience](#)
- [Hardware and Software Requirements](#)
- [Installing Inspector](#)
- [Registration](#)
- [Analyzing Digital Evidence](#)
- [Reporting](#)
- [Sharing Cases](#)
- [Backing Up Case Evidence](#)
- [Getting Support](#)

## Intended Audience

Forensic software tools offered by Cellebrite are intended for use by law enforcement officials, private investigators, corporate security specialists, and other parties who investigate Mac-based and Windows-based computers devices for evidentiary data.

Users of Cellebrite software should possess these core competencies.

- Basic knowledge of and experience using Apple and Windows computers and their peripheral devices
- Familiarity with macOS and Windows operating system environments
- Knowledge and training in basic computer forensics policies and procedures
- An understanding of forensic images and how to correctly acquire them
- A fundamental understanding of how to preserve, acquire, authenticate, and analyze digital evidence, and how to report digital forensic investigation findings



## Digital Forensics Overview

Forensics is preserving, acquiring, authenticating, analyzing, reporting, and managing digital evidence. Digital evidence includes data found on computer hard drives, external hard drives, CDs and DVDs, portable media such as USB thumb drives, Android devices, and iPod, iPhone, and iPad (iOS) devices.

A digital forensic examination includes these basic steps.

1. Preserve: Identify, secure, transport, and store the digital evidence (chain of custody).
2. Acquire: Create a forensically sound image of the evidence.
3. Authenticate: Confirm the forensic image is identical to the original (forensically sound).
4. Analyze: Create a case and analyze the evidence using an appropriate software solution.
5. Report: Thoroughly document the data investigation process and results of the analysis.
6. Manage: Back up, archive, detach/attach, and restore cases and evidence as needed.

## Preserving and Acquiring Digital Forensic Evidence

**Important:** Protocol for preserving and acquiring digital evidence varies according to local, state, and federal laws, and according to corporate policy. Be aware of such protocol before you begin a digital forensic investigation.

Digital evidence must be preserved in its original form to the greatest extent possible for it to be admissible during a legal proceeding. A forensic examiner must carefully preserve, acquire, and authenticate electronic data during their examination. Therefore, it is of the utmost importance to acquire electronic evidence in a way that ensures no changes are made to the original data during the acquisition process.

A forensically sound image is a bit-by-bit image that is identical in every way to the original, including allocated, unallocated, and free space.

### Preserving Evidence Using a Write-Blocker

Some operating systems attempt to write to the hard drive or device containing original evidence during the acquisition process. A write-blocker stands between the forensic examiner's computer or hardware acquisition tool and the devices containing the original evidence. Write-blockers prevent evidence contamination during the acquisition process.

**Important:** Always use a write-blocking hardware device or write-blocking software when acquiring digital evidence.

These are the types of write-blockers.

**Hardware-Based Write-Blockers:** A hardware-based write-blocker is a hardware device that is placed with cables and port connections between the forensic examiner's computer and the device containing the original digital evidence. Hardware-based write-blockers allow one-way, read-only data transfer between the device containing the evidence and the forensic examiner's computer. If the forensic examiner's operating system tries to write to the device containing the original data, the write-blocker blocks the unwanted data transfer.

**Software-Based Write-Blockers:** Software-based write-blockers serve the same purpose as hardware-based write-blockers. Software-based write-blockers reside on either the forensic examiner's computer, or on a hardware acquisition tool. SoftBlock™, offered by Cellebrite, is an example of a software-based write-blocker that runs on the forensic examiner's computer. Digital Collector, offered by Cellebrite, is an example of a hardware acquisition tool that has a software-based write-blocker built in.

A software-based write-blocker may be advantageous to a forensic examiner, as it may eliminate the need to purchase and carry expensive and cumbersome external hardware-based write-blockers.

**Important:** Be sure to test all write-blocking tools before performing an acquisition.

**Note:** For Mac computers, before you begin a forensic examination, you should also set .dmg files to read-only status as an additional safeguard. To do this, select the .dmg file(s), type COMMAND+L to open the Get Info window, and mark the **locked** checkbox.

### Using SoftBlock During a Live Acquisition

A forensic examiner may need to acquire data from a machine while the machine is running, or live. Data collected during a live acquisition may be saved to a forensic image as needed. Live data may be acquired from hard drives or another electronic data source.

During a live acquisition, the device containing the original evidence must remain connected to the forensic examiner's machine throughout the investigation. A write-blocker must be in place throughout the investigation as well. SoftBlock is an excellent software-based write-blocking solution for live data acquisitions.

## Acquiring Digital Evidence

A forensic image is a physical representation of the acquired device, even though it is saved as a file. Forensic images are static, meaning they remain the same even after you add them to a case. Forensic images may be backed up and stored for later use if necessary.

A forensic examiner uses these types of tools to acquire digital evidence.

**Hardware Acquisition Tools:** Hardware acquisition tools are physical devices used to collect digital evidence. They do not necessarily have a central processing unit (CPU), are self-contained, and may be hand-held. Digital Collector is an example of a hardware acquisition tool. Digital Collector can acquire a forensically sound image or collect data directly from a live source Mac or Windows computer (including RAM for macOS).

**Software Acquisition Tools:** Software acquisition tools reside on a forensic examiner's computer. Software acquisition tools often allow a forensic examiner to choose the forensic image file format, compression level, and the size of the data segments at the time the acquisition is performed. Inspector, offered by Cellebrite, has a software acquisition tool built in for acquiring iOS and Android devices.

## Authentication and Hashing

After you acquire a forensic image, you must authenticate it to confirm the image is an exact copy of the original. This is accomplished by hashing both the source and the acquired image. Hashing is the process, done by forensic software, of applying an algorithm (mathematical formula) to generate a value that uniquely identifies data. This value is usually expressed as a sequence of hexadecimal digits. If the hash value of the acquired forensic image matches the hash value of the original data, the forensic image and original data can be considered identical.

Digital Collector and Inspector use these algorithms to generate hash values.

- Message Digest 5 (MD5)
- Secure Hash Algorithm 1 (SHA-1)
- Secure Hash Algorithm 2, 256-bit length (SHA-256)

**Note:** You may also hash individual files with Inspector.

## Hardware and Software Requirements

The macOS installer for Inspector is delivered as a package file (.pkg) while the Windows installer is delivered as a setup executable.

In addition to the Inspector installers, installers for Operating System hash sets and memory symbols will need to be installed in order for Inspector to take advantage of those.

### Recommended Hardware Requirements

<b>Platform</b>	Intel 64-bit based systems
<b>Processor Requirements</b>	Intel Xeon E5, 6-Core, or better
<b>RAM Requirements</b>	32 GB DDR3 or higher
<b>Screen Resolution</b>	1680 x 1050 or higher
<b>Free Disk Space</b>	5 GB (installation only) 25 GB (temp space)

### Minimum Hardware Requirements

<b>Platform</b>	Intel based systems (Mac) x64 Architecture (Windows)
<b>Processor Requirements</b>	2.7 GHz Intel Core i7
<b>RAM Requirements</b>	16 GB DDR3
<b>Screen Resolution</b>	1024 x 768 or higher
<b>Free Disk Space</b>	5 GB (installation only) 25 GB (temp space)

## Minimum Software Requirements

<b>Operating System Specification</b>	Mac OS X 10.12.6 or newer*‡ Windows 10 1809 or newer Windows Server 2016 or newer
<b>iTunes</b>	12.6 or newer
<b>QuickTime (Mac)</b>	7.6.9 or newer
<b>Windows Media Player (Windows)</b>	12 or newer**

\* In testing it was determined that Inspector performs best on OS X version 10.14.6.

‡ We recommend strongly against using macOS versions .0 and .1 in all cases. For example, 10.15.0 or 10.15.1.

\*\*For Windows systems, Inspector uses whatever the default app may be for playing media files. Windows Media Player 12 is recommended. If you use Windows and do not have QuickTime installed and you need to play certain file types such as .AMR files (voicemail and so forth) you must install some non-default codecs, following the instructions found here:

<http://shark007.net/win8codecs.html>.

For information about downloading iTunes and QuickTime, please visit

<http://www.apple.com/quicktime/download/>

## Installing Inspector

This user guide does not include installation instructions. For installation instructions, log in to <https://www.community.cellebrite.com/s/support> and select the *Inspector Installation Guide* in Product Documentation.

## Registration

Inspector product license registration occurs at the time of payment and before the product is downloaded or shipped. Each license is bound to either a USB security device or a license key.

You may view your current registration information, check for product updates and download new product releases from within Inspector, or by visiting our website at

<https://community.cellebrite.com/>.

Each new Inspector product license includes a one-year license subscription. During this one-year subscription period, you will have full access to Cellebrite technical support, and the right to download and install currently licensed product updates and new releases for that product.

Please be sure to renew your product license subscriptions annually to continue receiving subscription benefits.

Customers in law enforcement may continue to use Inspector if the subscription is not renewed; however, subscription benefits are no longer available.

Customers in the private sector can no longer use Inspector if the subscription is not renewed.

## Analyzing Digital Evidence

Digital forensic analysis includes identifying meaningful evidence that will be included in the forensic examiner's report. This section briefly describes several Inspector features that help streamline this process.

### Hashing Individual Files

As mentioned in the previous section, hashing may also be performed on individual files. When a new case is created, or additional evidence is added to an existing case, Inspector gives an investigator the option of hashing all files as they are added. These hash values may then be used to verify file integrity, identify duplicate files, and identify both known and unknown file types.

Known and unknown file type identification is useful during a forensic examination. Known file types might be standard system files that a forensic examiner may wish to ignore, or they may be files known to contain illicit or dangerous materials. Unknown file types may warrant further investigation.

### Known File Hash Set Database

Inspector can use a Known File Hash (KFH) database when installed. This database allows a forensic examiner to quickly identify known file types in a case and determine whether certain files represent meaningful or insignificant evidence.

### Searching

Inspector includes multiple search features. A live or content search is a bit-by-bit comparison of a chosen search term against the entire evidence set in a case. This type of search may take longer to complete than an index search, but a live (content) search allows the examiner to search for non-alphanumeric characters and perform pattern searches (such as regular expressions and hexadecimal values). A smart index search searches an index created by Inspector of data residing in allocated space.

## Tagging

The Inspector tagging feature bookmarks meaningful evidence within a case. Evidence can be easily located and referred to once it is tagged. External “supplementary files” may be attached to tagged evidence, even if such files are not part of the current case. Tagged evidence can be incorporated into a report at any time during the investigation process.

## Reporting

Inspector provides uniquely flexible and intuitive reporting features that allow forensic examiners to create customized reports and export them to one of several standard file formats.

### Generating Reports

Inspector includes a report feature that allows convenient report creation and modification. Reports created within Inspector are searchable and can be exported to the .docx file format (compatible with Microsoft Word, Apple iWork, Pages, and LibreOffice), .html, .pdf, .csv, or .txt file formats. Custom logo and branding materials may also be incorporated into the examiner report.

For more information, see [Reporting](#).

## Sharing Cases

Inspector includes a portable case feature that allows examiners to generate a portable case file for a case reviewer. An Inspector Portable Case reader, available for macOS and Windows, can be distributed with the data exported into the portable case file. This reader does not require installation, does not require a software license, and provides an interface for the case reviewer to view files, filter data, perform searches, tag information, and generate reports.

For more information, see [Portable Cases](#).

## Backing Up Case Evidence

Throughout a digital forensic investigation, you should regularly make backups. Do this by copying the case to secure media and storing the media in a secure location.

When planning an investigation and determining the resources needed, ensure sufficient storage space is available to keep adequate backups of the case. Each case backup requires the same amount of drive space as the case itself.

## Getting Support

You can log in to MyCellebrite portal at <https://community.cellebrite.com>, which provides access to resources and support.

- Keep your products updated.
- Contact Support or review the knowledgebase.
- Download user manuals and data sheets.
- Manage your product licenses.
- Get expert assistance.

You can also send an email to technical support at [support@cellebrite.com](mailto:support@cellebrite.com).

These technical publications are available for download.

- *Inspector Quick Start Guide*
- *Inspector Installation Guide*
- *Inspector User Guide*
- *Inspector Portable Case Guide*



## Workspace Orientation

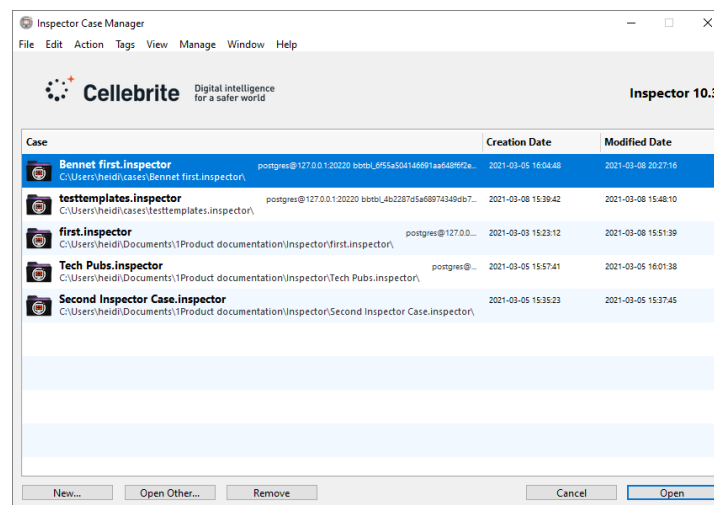
This chapter provides these topics about the workspace in Inspector.

- [Case Manager Window](#)
- [Case Info View](#)
- [Case Window](#)
- [Menu Bar](#)
- [Toolbar](#)
- [Component List](#)
- [Details View](#)
- [File Information Pane](#)
- [File Content View](#)
- [Managing List Views](#)
- [Settings, Preferences, and Options](#)

## Case Manager Window

Before you launch Inspector, make sure there is enough storage space on the working hard drive to store case files.

When Inspector is launched, the Inspector Case Manager window appears. Recent cases are listed in the Inspector Case Manager window.



The Inspector Case Manager window shows a list of recently opened cases. To open a case file, select the case and click **Open**. To reopen a case after it has been removed from the recent case list, click **Open Other**, navigate to the case file, and then click **Open**. You can open a case located anywhere in the file system.

- On Windows computers, double-click the case file in File Manager.
- On Mac computers, double-click the case file in Finder. You can also drag a case file from Finder onto the Inspector Case Manager window to add it to the recent case list.

To remove a recent case from the Inspector Case Manager window, select the case and click **Remove** or press DELETE.

If the Inspector license subscription is due to expire in less than 60 days, a notice appears near the top of the Inspector Case Manager window indicating the number of days until expiration.

If the subscription is not renewed, customers in the private sector can no longer use Inspector. Customers in law enforcement can continue to use Inspector after the expiration date, but software updates are no longer available.

If you attempt to open a case file created using a previous version of Inspector, a prompt appears. Click **Update** to update the case file. The case file updates and case information remains intact, but it is always a good idea to back up case files before you update, as a precaution.

**Note:** Some versions of Inspector do not support updating case files from previous versions.

For more information, see [Open a Case](#).

## Case Info View

On the toolbar, click **Case Info**. The Examiner Information and Case Information fields appear where you can provide information about the examiner and the case, such as the case number and case synopsis. You can change this information any time during the examination.

The screenshot displays the 'Case Info View' window, which is organized into three main sections:

- Examiner Information:** This section contains several text input fields for personal and professional details. The fields are labeled: Name (containing 'Technical Publications'), Organization (containing 'Where I Work'), Title (containing 'Examiner, Analyst'), Email (containing 'sample@email.com'), Address (containing 'Where I am'), Phone (containing '800-555-1234'), and Fax (containing '888-555-4321').
- Case Information:** This section contains three input fields: Number (containing 'B1'), Name (containing 'Bennet first'), and Synopsis (containing 'This is the synopsis').
- Case Time Zone Display:** This section features a dropdown menu for 'Time Zone' (set to 'UTC') and an 'Example' field showing a timestamp: '2021-03-05 23:14:07 (UTC)'.

The Examiner Information fields retain the information you provide when you create your first case in Inspector; you don't need to provide this information each time you create a case.

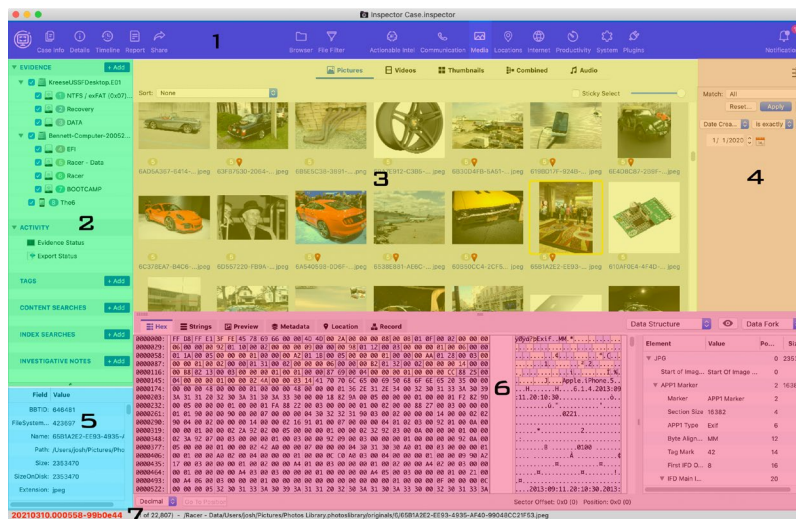
Because each case is unique, you must provide the case number, case name, and synopsis for each case in the Case Information fields. In the bottom left corner of the Case Info window, you may select a time zone in the **Time Zone** field. This determines the time zone used by evidence timestamps in the Case Window and in the examiner report.

By default, Inspector displays timestamps as Coordinated Universal Time (UTC). Dates and times are displayed with the selected time zone appearing in parentheses, for example: 2009-12-19 19:34:51 (PST). Inspector makes automatic adjustments for daylight savings time shifts for different parts of the world. You don't need to make any manual changes.

## Case Window

The Case window contains these elements.

1. Toolbar
2. Component list
3. Content pane
4. View filter
5. File Information pane (metadata)
6. File Content view
7. Status bar



## Toolbar

The toolbar is located at the top of the Case window and is used to select different views that display device data in the Content pane in various ways. Additionally, there are several Content pane sub-views. These sub-views are discussed in more detail later in this manual.

By default, the toolbar shows large icons and text labels. You can customize the toolbar by opening the toolbar context menu (press CTRL and select, or right-click anywhere on the toolbar).

The context menu for the toolbar has these options.

Option	Description
Big Icons with Labels	Default view with large icons and text labels
Small Icons with Labels	Small 16x16 pixel icons with labels
Big Icons	Large icons without labels
Small Icons	Small 16x16 pixel icons without labels
Labels Only	Shows text labels without icons

## Component List

When you add a device to a case, it is listed in the Evidence section of the Component list. Select the disclosure triangle next to a device to view device partitions and carved files located in unallocated space. To add evidence to a case, to the right of Evidence click **Add** and select the evidence type.

The Activity section of the Component list shows file export status and evidence status (data import and processing status). Progress indicators appear here for many Inspector- user-initiated tasks.

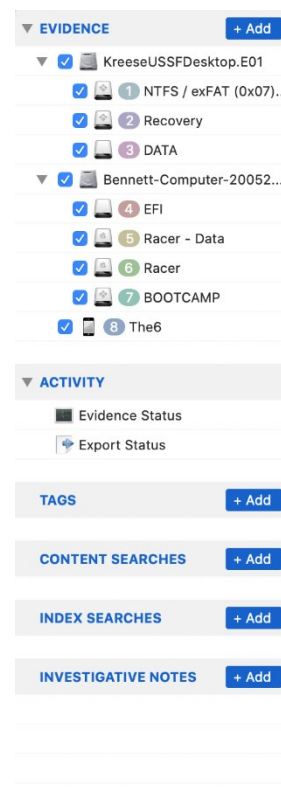
Search results and the search criteria used for saved searches appear in the Content Searches section of the Component list. An examiner may create several custom searches during an examination, save them, and later refer back to the results and settings for each at any time during an examination.

Queries created for Smart Index appear in the Index Searches section of the Component list. An examiner may create and save multiple index queries during an examination, save them, and later refer back to the results at any time during an examination.

Tags and tagged items appear in the Tags section of the Component list. Select a tag to view individually tagged items within the tag. The numeric badge to the right of each tag indicates how many tagged items are contained within the tag.

Investigative Notes appear in the Investigative Notes section of the Component list. Investigative Notes can be added by at any time during an examination.

For more information, see [Component List](#).



## File Information Pane

Select a file and click the **File Information** pane to display metadata associated with that file. If the selected file is an image file, additional metadata is likely present.

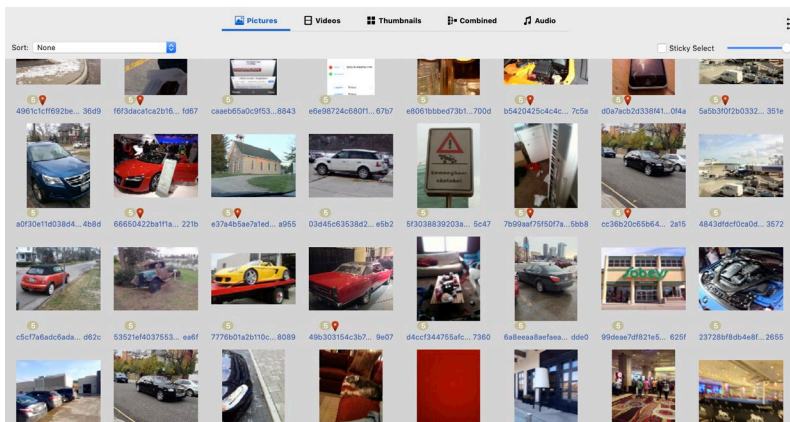
Field	Value
<b>Main</b>	
BlackLight ID:	36903
Evidence ID:	45
File System ...	8590668587
Name:	flt4.gif
Path:	/usr/share/doc/ntp/pic/flt4...
Size:	3876
Size On Disk:	3876
Owner ID:	0
Group ID:	0
Permissions:	292
Extension:	gif
Content Ext...	GIF
Date Created:	2017-05-05 00:21:03 (U...
Date Modifi...	2017-05-05 00:21:03 (U...
Date Acces...	2017-05-05 00:21:03 (U...
Date Chang...	2017-11-29 20:30:34 (???)
Locked:	No
Hidden:	No
Fork Count:	1
File System ...	APFS
<b>Location O...</b>	
Extents:	1
Physical Se...	100640160
Logical Sect...	100230520
Logical Clus...	12528815

The File Information pane displays extended attributes, hash values, date and time stamps, file paths, file size and EXIF, TIFF and location (GPS) data. Drag the dot at the top center of the File Information pane up or down to adjust the pane size.

To hide and show the File Information pane, on the menu bar click **View > Hide File Info** or **Show File Info**.

## Content Pane

The Content pane displays data in various ways depending on which view option or Component list item you select. In the Component list, select which devices to view by marking the checkbox next to the name. From left to right, select each toolbar button to navigate through the different Inspector view options. In the Component list, from top to bottom, select Activity, Content Searches, Index Searches, and Tags to see how the Content pane displays each.

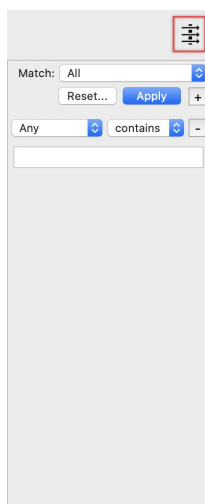


A numbered badge appears in each view representing the numbered evidence item from the Component list.

An examiner works with the Content pane the majority of the time during forensic analysis. The Content pane displays data as a file list the majority of the time.

## View Filter

The view filter exists in certain views such as the Media view. This filter allows for specific filtering of the data within the current view only. To see the view filter, click the **Show/Hide Filter** button.



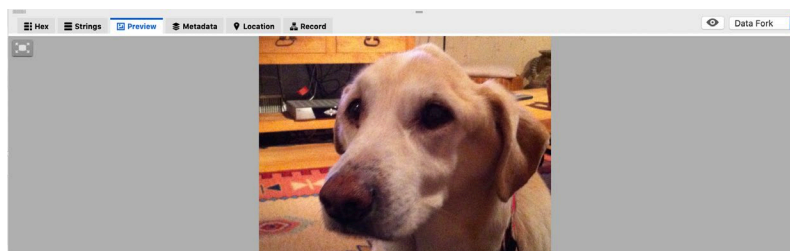
If the filter is active (applied) the Show/Hide Filter button is green.

## File Content View

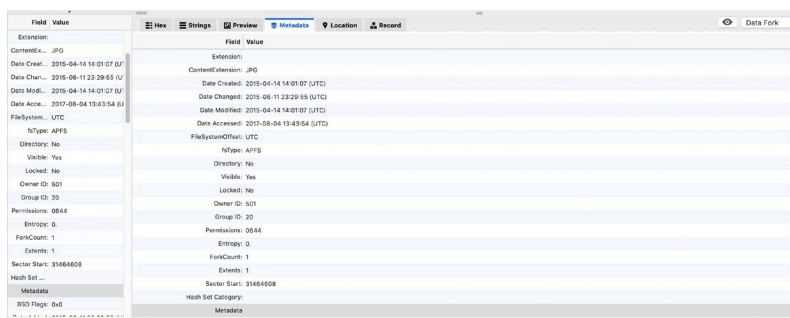
The File Content view has these main file viewing options.

- Hex
- Strings
- Preview
- Metadata
- Location
- Record

In the Content pane, select a file. At the top of the File Content view, click **Hex**, **Strings**, and **Preview** to view the file as hexadecimal data, as character strings, and as a rendered preview, respectively.

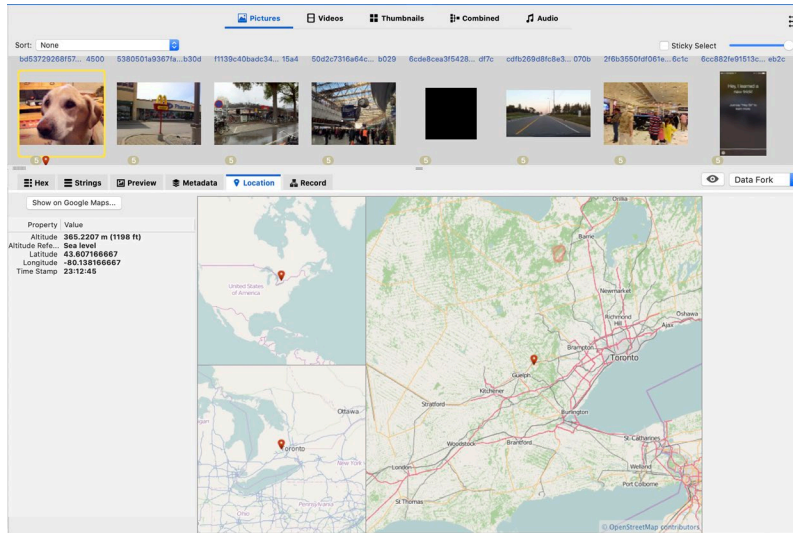


With a file selected, click **Metadata** in the File Content view. The metadata contents shown are identical to those displayed in the smaller File Information pane to the left, but you can enlarge the pane as much as you wish.

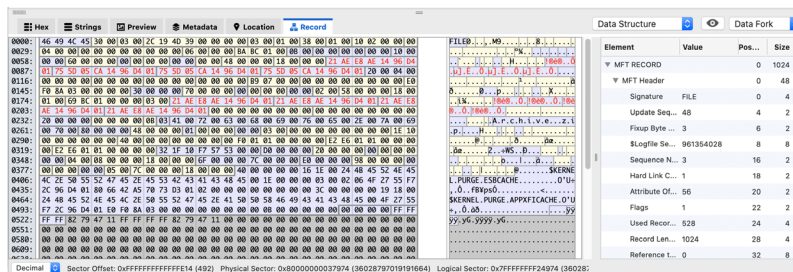




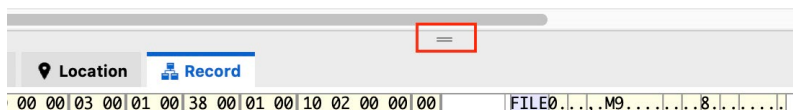
Select any media file that contains geolocation (GPS) data (as indicated by a red placemark icon), or any applicable record in the Location view, then click **Location** in the File Content view to display one or more offline maps depicting the item's latitude and longitude coordinates. Inspector also has a button to optionally view the location in Google Maps (if connected to the Internet), and other geolocation information contained in the file's metadata.



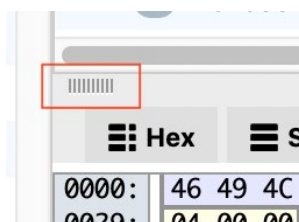
Any selected file which exists on a filesystem that has a record system like HFS and NTFS (Catalog Tree, and MFT respectively), will display the file record.



To adjust the size of the File Content view, at the top of the pane, click and drag the handle up or down.



You can "tear off" the File Content view as a separate window so you can simultaneously see the file content in multiple windows. The tear-off handle appears as several short, vertical lines immediately above the Hex tab in the File Content view.



Click the handle and drag it away in any direction. A new File Content view window appears. This new window can be placed on another monitor if multiple monitors are being used, and it can be enlarged to the desired size. Additional tear-off File Content view windows can be created, and each one can be used to view different data if desired. For example, one window may show the Preview tab, while another shows Metadata, and a third reveals Location maps. When a file is selected within the original case window, such as in Browser view, all of the tear-off windows update to reflect information related to that file. There is no need to reconnect these tear-off windows to the original case window. Simply close each window when finished with it. Even though the File Content view can be hidden on the original case window, it is always there and never has to be reattached.

For more information, see [File Content View](#).

**Note:** The File Content view pane is not active in Case Info, Details, Report, and Share views.

## The Status Bar

The Status Bar shows selected data such as Content pane file counts and the pathnames of selected files pathnames. Some progress bars also appear in the Status Bar.

## Menu Bar

The menu bar in Inspector is located at the top of the screen on a Mac computer and at the top of the application window on a Windows computer. The menu bar has these options.

Option	Mac	Windows
Inspector	✓	
File	✓	✓
Edit	✓	✓
Action	✓	✓
Tags	✓	✓
View	✓	✓
Manage	✓	✓
Window	✓	✓
Help	✓	✓

**Note:** Only Inspector for Mac includes the Inspector menu. This is due to the difference between the Mac and Windows platforms.

## Inspector Menu

The Inspector menu is available only on Mac computers.

In the menu bar, click **Inspector**, and then click the appropriate action.

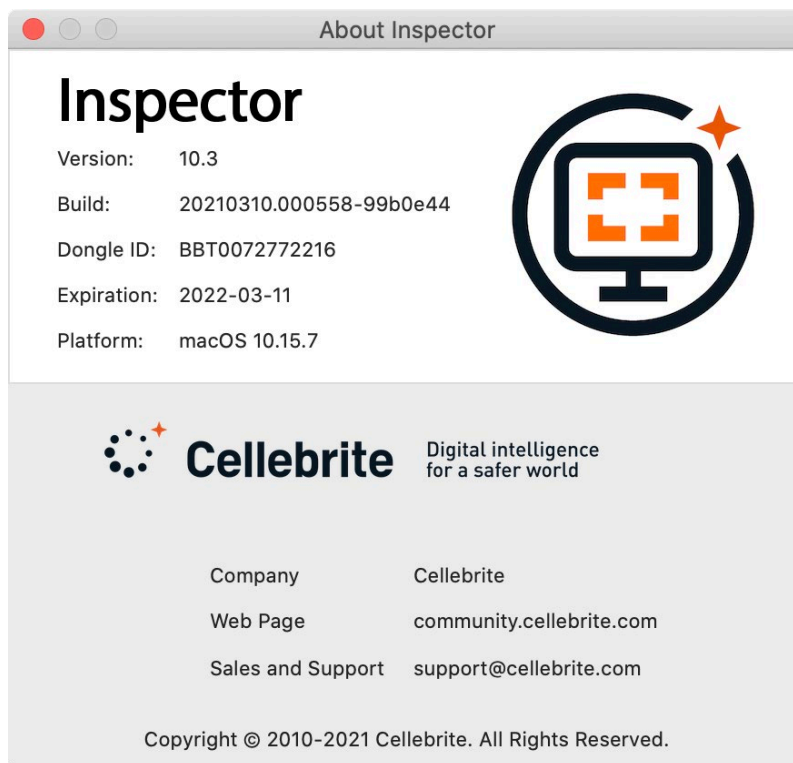
Option	Description
About Inspector	Version, license, and contact information for Inspector
Check for Updates	Check for a newer version of Inspector
Preferences	Open the Inspector preferences window. For more information, see <a href="#">Inspector Preferences or Options</a> .
Services	Open System Preferences Keyboard shortcut service
Hide Inspector	Hide the Inspector application window
Hide Others	Hide all other application windows except Inspector
Show All	Show all application windows
Quit Inspector	Stop and exit the application

## About Inspector

The About Inspector option opens the About Inspector window, which shows dongle ID (serial number) and license expiration.

Please have the Dongle ID ready when contacting Cellebrite Technical Support or your sales representative. The expiration date shown is the date when the Inspector License Subscription (BLS) contract ends.

For public sector customers, Inspector continues to function after the BLS expiration date, but software updates are no longer available. For private sector customers, Inspector no longer functions after the BLS expiration date.



## Check for Updates

The Check for Updates option is available if the analysis computer has an Internet connection. Select this option to see if new updates are available. A web browser opens to the [MyCellebrite portal](https://my.cellebrite.com), where you can log in and navigate to the Inspector software downloads page.

## File Menu

Select the **File** menu and choose the appropriate submenu option to create a new case, open an existing case, or add evidence such as disk images, devices, and folders to a case.

The File menu contains these items.

Option	Description
New Case	Create a new Inspector case
Open Case	Open an existing case
Open Recent	List recently opened cases
Close	Close the current case
Add Evidence	Add evidence to the case
Add Selected	Add selected evidence (such as a selected disk image) to the case
Create Case Archive	Create an archive of a case from the Case Manager window for transfer between Mac and Windows platforms
Restore Case Archive	Import a case archive into a new casefile
Save Case Template	Save customized case settings (tags, file filter, search, and evidence import settings) as a processor template
Import Case Template	Import a case template containing customized case settings and apply it to a new case
Export Case Template	Export a case template (for other examiners to use)

## Create Case Archive

To move a casefile between computers with different platforms, such as one created on a Mac computer to a computer running Windows (or vice-versa), a case archive must be created, which can then be transferred between the two computers. A case archive can also be used to import a case file into a version of Inspector that does not support upgrading case files from previous versions of Inspector.

To create the case archive, navigate to the Case Manager window, click **File > Create Case Archive**. A Save window appears, allowing the examiner to choose where to save the archive. The archive is comprised of a folder containing a *bl-casedata* text file and a *partitions.zip* archive. When transferring the archive between computers, the folder and its contents must be copied.

## Restore Case Archive

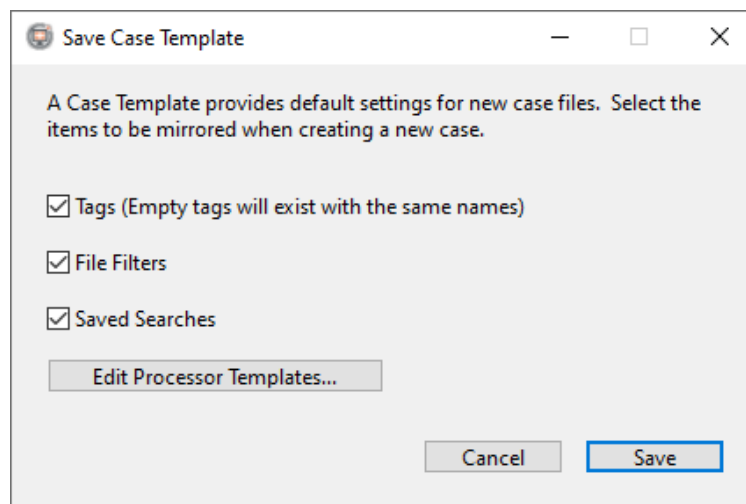
To open a case archive, the archive must be imported into a new casefile.

To import the archive folder, navigate to the Case Manager window, click **File > Restore Case Archive**. An Open window appears. Within this window, select the archive folder containing the *bl-casedata* text file and *partitions.zip* file, and then click **Open**.

## Save Case Template

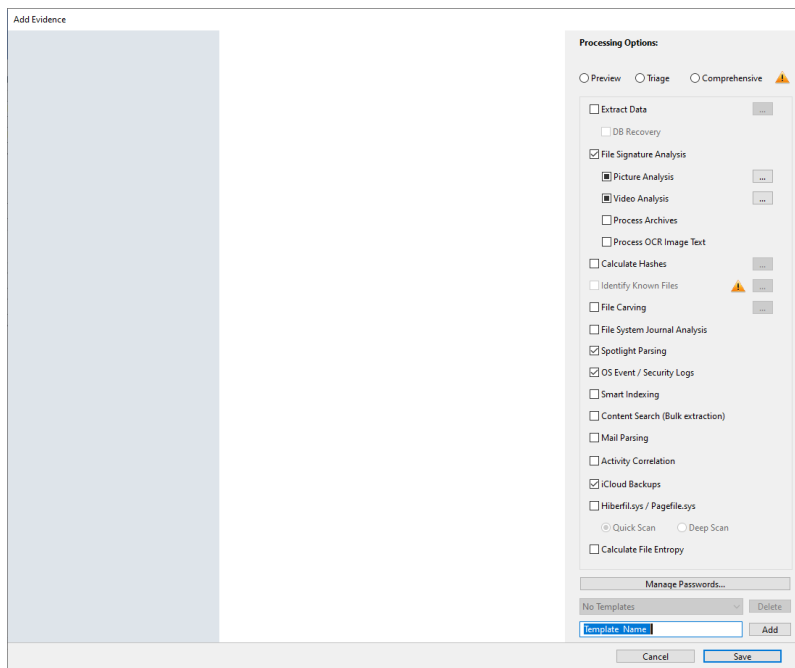
Customized Inspector case settings such as tags (empty), file filters, saved searches, and evidence processing options can be saved to a template and used in subsequent cases.

To save the current settings as a template, click **File > Save Case Template**. The Save Case Template window appears, where you can choose which settings to include in the template.



Click **Edit Processor Templates**. The Add Evidence window appears, with no evidence shown.

Choose the processing options to save, then in the field below all the processing options, type the name for the processor template, and then click **Add**.



The new processor template is added to the Saved Templates list. To delete a processor template, select it in the Saved Templates list and click **Delete**. When finished, click **Save**. Then click **Save** in the Add Evidence window.

For more information, see [Adding Evidence to a Case](#).

For using a saved case template (for example a template with saved tags, file filters, and saved searches), you need only create a new case. The saved settings are automatically reflected by default in the new case, even if the Inspector application was restarted since the settings were saved.

## Export Case Template and Import Case Template

To share a template with other examiners, the template must be exported (as opposed to using the Save Case Template option). Likewise, to save multiple case templates, export each one by clicking **File > Export Case Template**. To finish the export process, type the name of the template, choose the save location, and then click **Save**.

To import a case template, click **File > Import Case Template**, select the appropriate template, and then click **Open**.

## Edit Menu

The Edit menu includes typical cut, copy, paste, undo, redo, and find submenu options.

In the Search Results view (such as when an item is selected in the Content Searches section of the Component list), the Edit menu includes the Delete Search (search name) option.

In the Tags view (such as when an item is selected in the Tags section of the Component list), the Edit menu includes the Delete Tag (tag name) option.

On the Windows platform, the Edit menu includes Options, which is identical to Inspector > Preferences on the Mac platform. For more information, see [Inspector Preferences or Options](#).

## Action Menu

The **Action** menu includes several options for handling evidence.

Option	Description
Save File Listing	Save attributes from the selected file(s), such as date stamps, paths, extensions and File IDs, to a text file
Copy Path	Copy the selected file's path to the clipboard
Quick Look (Mac only)	Preview the selected file without launching its application
Find Identical Files	List all files with identical hashes to the selected file(s)
File History	Display a File History window for files with variants parsed from Windows Volume Shadow Copies
Export	Provides access to a sub-menu for exporting information from Inspector
Reveal	Provides access to a sub-menu for revealing data

## Save File Listing

The Save File Listing menu option saves attributes for the selected files (such as date stamps, paths, extensions, and unique IDs) to a text file. When you click Save File Listing, the Save dialog box appears. Select the location where the new case should be saved, and then click **Save**.

By default, Inspector File Listings are saved as .asc files, which may be opened by a text editor or spreadsheet application.



## Copy Path

The Copy Path menu option is only available when a file is highlighted. This feature copies the selected file's path to the clipboard. The Copy Path option is useful when using the Search feature in the Contain Search to area. Simply copy the path into the search path text field.

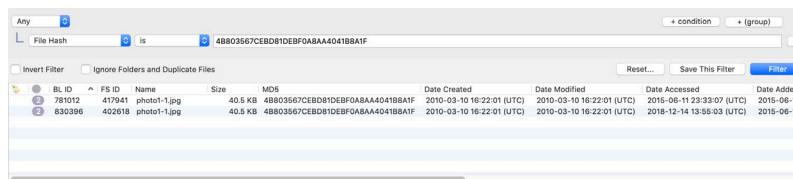
## Quick Look

The Quick Look menu option is available only on Mac computers. It opens selected file using the Apple Quick Look framework. Quick Look renders the selected file in its native view if there is an appropriate Quick Look plug-in, or the file's native application is installed on the examiner's analysis machine.

Highlight a file and press SPACEBAR to activate the Quick Look feature via keyboard shortcut.

## Find Identical Files

To locate files with the same hash value as a specific file (identical files), select a file in the Content pane, then click **Find Identical Files**. Inspector automatically switches to the File Filter view and applies the List All Files and File Hash | is | <hash value> filter options. Files with the same hash value appear in the Content pane.



## File History

The File History menu option is available only when files from a Windows volume with Volume Shadow Copy variants are selected or highlighted. When a file is selected and the File History menu option is chosen, a File History window appears.

For more information, see [Browser View](#).

## Export Menu

The Export menu option is used to export selected or highlighted files. The Export menu opens a sub-menu with several export options:

Option	Description
Export Selected Files	Export (copy) the selected file(s) to an external folder
Export Selected Files As L01	Export the selected file(s) to a Logical Evidence File maintaining metadata and folder structure
Export for Legal Review	Export responsive files while preserving important metadata
Export Hash Set	Export hash values for all selected files as an Inspector hash set (Inspector hash sets can be saved and imported into other Inspector cases)
Export Data Model	Export selected files to the chosen data model format
Export Case Data As XML	Export case data (all evidence items or a selected evidence item) to an XML file
Export Selected Rows	Export selected database rows from the active case to a tab-delimited or CSV file
Export Selection	Export a highlighted selection as either raw, formatted data, or as simple hex
Export Selected Location Data As	Export GPS metadata from selected files to a KMZ or KML file (Google Earth placemark file)

Some menu selections have additional sub-menus.

### Export Selected Files

These are the options in the Export Selected Files menu.

- Files Only
- Folder Structure
- Folder Structure (from root)

The Files Only options exports only the selected files. If a folder is selected, the files within the folder will be exported, but the folder will not be exported. The files from the folder will be placed in the directory chosen for export along with any other files selected for export. If files are selected from more than one device or volume they will all be placed in the same export folder. Refer to the Volume Name or Volume ID in the *\_BBTExportLog.txt* to determine on which device or volume the files were originally located.

The Folder Structure option exports selected files and folders. When folders are selected, the folders and the files within the folder will be placed in the directory chosen for export along with any other files selected for export. If files are selected from more than one device or volume, a

folder will be created in the export directory named with the number badge shown in the Component list, underscore, device, or volume name. The files and folders exported from each device or volume will be placed in the corresponding folder.

The Folder Structure (from root) option exports the selected files and folders, maintaining the folder structure from the root of the device. If files are selected from more than one device or volume, a folder will be created in the export directory named with the number badge shown in the Component list, underscore, device, or volume name. The folder structure from the root of the device or volume will be created in the corresponding export directory containing the files and folders selected for export.

## Export Selected Files As L01

The Export Selected Files As L01 menu option is available only when files are selected or highlighted. When a file is selected and you choose the Export Selected Files As L01 option, you can select or create a destination folder and provide a name for the Logical Evidence File.

## Export For Legal Review

Click **Export for Legal Review** to export selected files in a format suitable for loading into an electronic discovery review platform. From any file list, select the files to export and choose **Export for Legal Review**. The Export Files for E-Discovery dialog box appears. In the Load File Format field, select the appropriate load file type. Type the custodian ID, custodian name, and a case name into the corresponding text fields.

Cases can be exported to an Inspector Load File, a tab-delimited file, or a Concordance load file. Options are also available in the Export Files for E-Discovery dialog to add a prefix to the collection folder name and the files. The folder name is a combination of the Folder Prefix and the Case Name.

Export Files for E-Discovery

Load File Format: Inspector Load File

Custodian ID: 9421

Custodian Name: Smith

Case Name: 0001

CAPTURE0001/

DOCUMENT000000001

Folder

Prefix: CAPTURE

Starting ID: 1

Length: 4

Files Per: 5000

File

Prefix: DOCUMENT

Starting ID: 1

Length: 9

☒ Add missing file extensions (file typing required)

☒ Ignore .DS\_Store files

Cancel Save

Files in the capture are named using the File Prefix. There are also options to Add missing file extension (file typing required) and to Ignore .DS\_Store files.

When settings are complete, click **Export**. A load file containing the selected files and information about the files (metadata) is generated. Once files are exported to a destination folder, if an attempt to create a second export in that folder is made Inspector provides a warning. The warning is an effort to prevent overwriting previous exports.

## Export Hash Set

Custom Inspector hash sets (.blhs) may be saved and imported into other Inspector cases. To generate a hash set from specific files in any Inspector view, select the files and click **Export Hash Set**. The Hash Set Export dialog box appears, presenting the three hash types: MD5, SHA-1, and SHA-256. Mark the hash types to include in the hash set, and then click **Continue**. In the Hash Set Save Location dialog box, click **Save**. The custom Inspector hash set is generated and saved.

To generate a hash set of every file in a case, in the Browser view, select the root folder (at the top of the file list) and choose the **Export Hash Set** menu option.

By default, hash sets are saved in the */Cellebrite/Inspector/Hash Sets* folder. This folder is found in these locations.

- macOS: *User/Library/Application Support/Cellebrite/Inspector/Hash Sets*
- Windows: *\user\AppData\Roaming\Cellebrite\Inspector\Hash Sets*

You may also import existing custom Inspector (.blhs), EnCase (6.19 and lower), and NSRL hash sets, as well as hash sets saved as plain text documents. For more information, see [Hash Set and File Signature DB Management](#).

## Export Data Model

The Export Data Model menu option is used to export images, videos, and thumbnails in a specific data model format. Data models for pictures and videos can be exported to LACE, C4ALL, Project Vic, and Semantics21 formats. When exported, these data models can be ingested into their respective utilities for further processing.

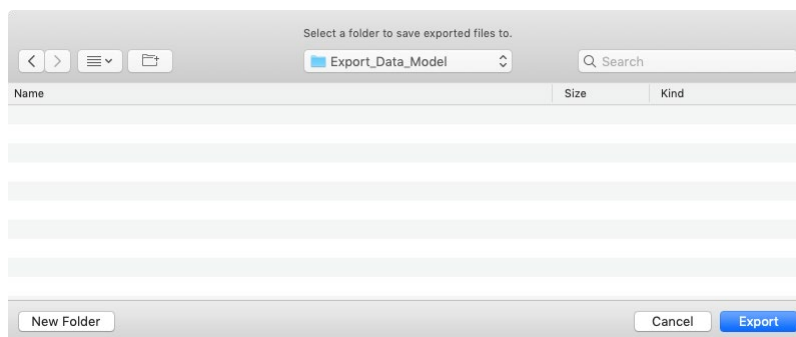
Before exporting the data models, Inspector must have completed these processes.

- Hashes
- Filetypes
- Pictures and/or Videos

The data model formats available are displayed in the sub-menu of are three options in the Export Data Model:

- Project VIC Version 1.1
- Project VIC Version 1.2
- Project VIC Version 1.3
- Project VIC Version 2.0
- BlueBear LACE
- C4ALL (For more information, see [C4All](#)).
- S21

To export to a given data model, select the files of interest and then click **Action > Export Data Model** followed by the preferred data model. A window appears to specify a destination folder. Once the folder is selected click **Export**.



## Export Case Data As XML

To export casefile data to an XML file, click **Export Case Data As XML**, and choose either **All Evidence Items** or **Selected Evidence Item**. This will generate an XML file containing all of the normalized data from the casefile for either all evidence items or the currently selected evidence item.

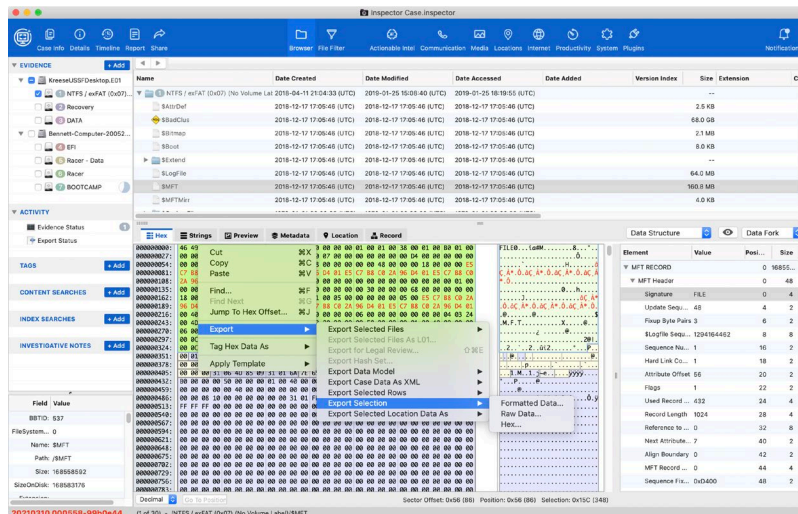
All normalized data from a Inspector casefile can be exported into a single XML file for ingestion into another utility that supports Inspector's XML format. Casefiles containing multiple pieces of evidence can export XML data for individual evidence items or for all evidence items.

## Export Selected Rows

The Export Selected Rows menu option is available from any view that displays data as a file list. This option may be used to export selected entries to either a TSV file, a Comma Separated Values (CSV) file, or logical evidence file (L01) depending on examiner preference. You can access this menu option from the **Action** menu or by opening the context menu for the selected rows.

## Export Selection

To export a Hex snippet from the File Content view as raw data, formatted data, or hex, at the top of the File Content view, click **Hex > Export Selection**. You can also open the context menu for the selected hex string and click **Export Selection**.



## Export Selected Location Data As

Files containing GPS information can be selected, exported to a .kmz or .kml file, and mapped with the Google Earth application.

1. Select file(s) containing GPS data, click **Action > Export Selected Location Data As**, and then choose either KMZ or KML format.
2. In the Export dialog box, type a file name and choose or create a destination folder, and then click **Export**.  
Inspector exports the GPS data to a .kmz or .kml file in the destination folder.
3. Open the .kmz or .kml file in Google Earth.  
Google Earth displays a pushpin for each file. Each pushpin is also listed in the Google Earth sidebar Places section.

To see an applied .kmz/.kml file usage example, see [Locating Live Victims](#).

## Reveal

Option	Description
Reveal File on Disk	Export the selected file(s) from the current case and reveal the new location in the Finder or system browser
Reveal File in File Browser	Reveal the file location within the Inspector Browser
Quick Look (Mac only)	Reveal the file location within the Inspector Disk View

### Reveal File on Disk

The Reveal File on Disk menu option exports (copies) the selected file(s) from the current case and reveals the new location in Finder or File Explorer. In the confirmation dialog box, click **View File(s)**, and then select a destination folder. Click **Export** to export the files to the selected destination folder. A Finder or File Explorer window opens to reveal the location of the exported files.

### Reveal File in File Browser

The Reveal File in File Browser menu option reveals a file's location within the Inspector Browser view. This feature is extremely useful. Select a file in the Inspector File Filter or Search view and then click **Reveal File in Browser**. Inspector switches to Browser view and displays the file in its actual location within the file system.

### Reveal File in Disk View

The Reveal File in Disk View menu option reveals a file's location within the Inspector Disk View. Select a file in the Inspector Browser or File Filter view and then select **Reveal File in Disk View**. Inspector switches to Details view, with the **Disk View** tab selected, and displays the file in that view.

## Tags Menu

The Tags menu contains options to help you manage meaningful evidence within a case. Tagged evidence is easily located and can be incorporated into the examiner's report at any time during the forensic examination.

Option	Description
Delete Selected Tag	Removes the selected tag from the case. All tags associated with the tag are also removed.
Tag <Type of Items> As	Adds the selected items to a new or existing tag.
Remove <Type of Item> From Tag Group	Removes the selected items from all tags or specified tags.

### Delete Selected Tag

This menu option is available when a tag is selected in the Tags section of the Inspector Case window.

**Warning:** Selecting this option deletes the selected tag and any tagged items associated with the tag. This action cannot be undone!

### Tag <Type of Items> As

This menu option lets you add selected objects to either a new tag or an existing tag. This name of this menu option changes depending on the context and on the objects that are selected.

- When a file or multiple files are selected the name is Tag File As.
- In the Actionable Intel tab, if Trash Items are selected the name is Tag Trash Items As.
- In the Actionable Intel tab, if User Accounts are selected the name is Tag User Accounts As.

Existing tags appear in the Tag <Type of Items> As menu along with their shortcut keys.

Option	Description
New Tag	Create a new tag for the the selected item.
Tag 1	Existing tag named Tag 1. Inspector automatically assigns the shortcut 1 to the first existing tag.
Tag 2	Existing tag named Tag 2. Inspector automatically assigns the shortcut 2 to the second existing tag.

For more information, see [Tags](#).



## Remove <Type of Items> From Tag Group

This menu option allows you to remove tagged items from all tags or a specific tag. This option is available when tagged items are selected in any view within Inspector.

**Warning:** This action cannot be undone!

Option	Description
All Evidence Tags	If selected items are listed in more than one tag, choosing this will remove the items from all tags.
<Tag Name 1>	Name of the first tag selected items are tagged in.
<Tag Name 2>	Name of the second tag selected items are tagged in.

When the selected items are tagged in multiple tags, all of the tags are listed.

## View Menu

The View menu provides these options.

Option	Description
Adjust List Columns	Choose which columns are visible in the list views, and change the order in which columns are displayed
Hide File Info / Show File Info	Hide or show the File Information pane, which provides metadata

## Adjust List Columns

To change the visible columns settings, click **View > Adjust List Columns**. You can show or hide each item in the list marking or unmarking its checkbox. You can also reorder items in this list by dragging and dropping each item in the list to the appropriate order. When you have finished making changes, click **Apply Changes**. The columns now appear in the specified order.

To return columns to the way they were displayed by default, click **View > Adjust List Columns**. Click **Reset List to Defaults**, then click **Apply Changes**.

**Note:** Column options vary depending on which view is selected, and Inspector applies column option settings to each view independently.

## Hide/Show File Info

To hide or show the File Information pane, click **View > Hide File Info** or **Show File Info**.

## Manage Menu

Use the Manage menu to manage hash sets, file signatures, plugins, C4All, SEMANTICS21, and passwords.

Option	Description	Mac	Windows
File Signatures	Open the File Signature Management window	✓	✓
Hash Sets	Open the Manage Hash Sets window	✓	✓
Plugins	Open the Manage Plugins window	✓	✓
C4All	Open the Manage C4All window	✓	✓
S21	Open the Manage S21 window	✓	✓
Passwords	Open the Passwords window	✓	✓
Drive Mappings	Maps to a volume letter of your choice, thus avoiding the file path character limit of Windows		✓

For more information, see [Hash Set and File Signature DB Management](#).

## Window Menu

Use the Window menu to manage your case windows.

You may find it useful to see two or more current case views simultaneously, such as tagged items within a tag and the examiner report.

Option	Description
Cases Window	Open the Inspector Case Manager window
Minimize	Minimize the current Inspector window
Zoom	Adjust current Inspector window size
New Window For This Case	Open another Inspector window for the same case
Hide Toolbar and Sidebar	Hide or show the Inspector toolbar, Component list and File Information pane

Open cases and multiple case windows appear as submenus in the Window menu. To bring a case to the front, click **Window** and select an open case.


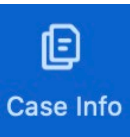
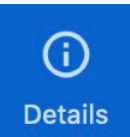
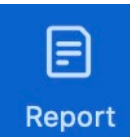
## Help Menu

Use the Help menu to get help, provide feedback, get technical support, and quickly access the Cellebrite website.








Option	Description
User's Guide	Open this manual
Cellebrite Website	Open the Cellebrite home page in a web browser
Inspector Feedback	Send an email to Cellebrite to provide feedback about Inspector
Technical Support	Open the technical support page on the Cellebrite website in a web browser
License Manager	Opens Inspector License Manager application
Enter License Manager	Opens Dongle Required window

## Toolbar

The toolbar provides access to information about a case, details about the evidence in a case, report features, the Inspector portable case feature, analysis tabs, and notifications from Inspector.

Button	Description
	Opens the Case Manager window. For more information, see <a href="#">Case Manager Window</a> .
 Case Info	Click <b>Case Info</b> to see details about the case, including Examiner Information, Case Information and Case Time Zone Display. For more information, see <a href="#">Case Info View</a> .
 Details	Click <b>Details</b> to see details about the selected device or partition and an interactive graphical representation of device contents. For more information, see <a href="#">Details View</a> .
 Report	Click <b>Report</b> to see, edit, and generate the examiner report. For more information, see <a href="#">Reporting</a> .

Button	Description
 Timeline	<p>Click <b>Timeline</b> to open the Timeline view.</p> <p>For more information, see <a href="#">Timeline View</a>.</p>
 Share	<p>Click <b>Share</b> to share the examiner report using the Portable Case feature.</p> <p>For more information, see <a href="#">Portable Cases</a>.</p>
 Browser	<p>Click <b>Browser</b> to see a view to navigate manually through the file structure on the device, similar to Finder on Mac computers or File Explorer on Windows computers.</p> <p>For more information, see <a href="#">Browser View</a>.</p>
 File Filter	<p>Click <b>File Filter</b> to quickly isolate specific files by kind or attribute.</p> <p>For more information, see <a href="#">File Filters</a>.</p>
 Actionable Intel	<p>Click <b>Actionable Intel</b> to see sub-views pertaining to the user's program execution (including Windows jump lists), device connections, device backups, account usage, file downloads, file knowledge (like recent items, Windows link files, and trash), passwords (Apple keychains), and searches.</p> <p>For more information, see <a href="#">Actionable Intel View</a>.</p>
 Communication	<p>Click <b>Communication</b> to see sub-views containing calls, messages, posts, voicemail, voice memos, favorites, contacts, and email. This includes data parsed from SMS, iMessage, and messages from other communication apps such as Skype, WhatsApp, Textfree, Kik, and so forth.</p> <p>For more information, see <a href="#">Communication View</a>.</p>
 Media	<p>Click <b>Media</b> to see and sort all pictures and video files located on devices, in folders, or recovered from unallocated space in Gallery view. Audio files may also be found in the Media view.</p> <p>For more information, see <a href="#">Media View</a>.</p>
 Locations	<p>Click <b>Locations</b> to see data parsed from maps applications, files containing location data, Wi-Fi networks, and location services data.</p> <p>For more information, see <a href="#">Locations View</a>.</p>

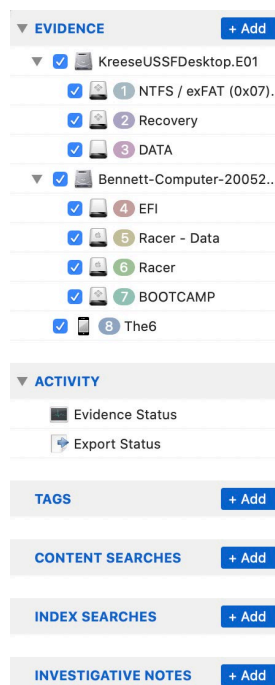
Button	Description
 Internet	<p>Click <b>Internet</b> to see internet history and cache information for Safari, Firefox, Chrome, Internet Explorer, and Edge browsers.</p> <p>For more information, see <a href="#">Internet View</a>.</p>
 Productivity	<p>Click <b>Productivity</b> to see data from the Calendar and Notes applications (macOS and iOS).</p> <p>For more information, see <a href="#">Productivity View</a>.</p>
 System	<p>Click <b>System</b> to see specific system files (including Windows registry items), data from Spotlight (macOS), data from a device's dynamic dictionary database, information about installed applications (includes profile information for installed social media apps), data from system logs, and memory parsed from memory files or Windows hibernation files.</p> <p>For more information, see <a href="#">System View</a>.</p>
 Plugins	<p>Click <b>Plugins</b> to see data parsed by any Inspector plugins for the selected devices. Inspector supports Apple Pattern of Life Lazy Output'er (APOLLO), a python script used to query data from iOS databases.</p> <p>For more information, see <a href="#">Plugins View</a>.</p>
 Notifications	<p>Click <b>Notifications</b> to see notifications, and copy their text and dismiss them. A badge indicates the number of unread notifications.</p>
 	<p>Show/Hide Filter appears just below Notifications, and only for views that allow you to filter data directly. Click <b>Show/Hide Filter</b> to toggle between showing and hiding the filter pane.</p> <p>The arrows are green when a filter is applied in the current view</p> <p>For more information, see <a href="#">File Filters</a> and <a href="#">Filtering within Specific Views</a>.</p>

## Component List

The Component list includes these sections.

- Evidence
- Activity
- Content Searches
- Index Searches
- Tags
- Investigative Notes

These sections are always present in the Component list; however, items listed under each Component list section change according to user actions and evidence added or deleted.



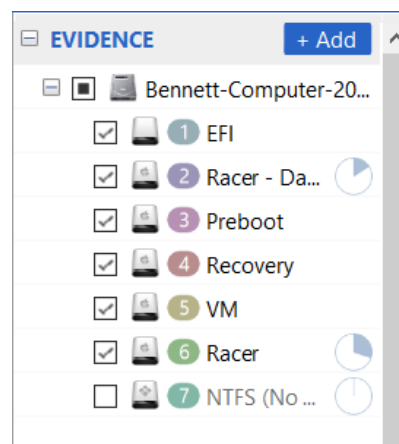
## Evidence

In the Evidence section of the Component list, you can see a hierarchical device list. When you acquire a device, the new device is added to this list. A hard drive icon represents data imported from a disk image. Mobile device icons display according to the type of source device type (such as Android, iPhone, iPad, or iPod). In the Evidence section of the Component list, select a disk image. The disk image partitions and partitions containing carved files in unallocated space are shown. When multiple pieces of evidence have been added to a case file, you can reorder evidence items by highlighting a specific item and dragging it up or down in the list.

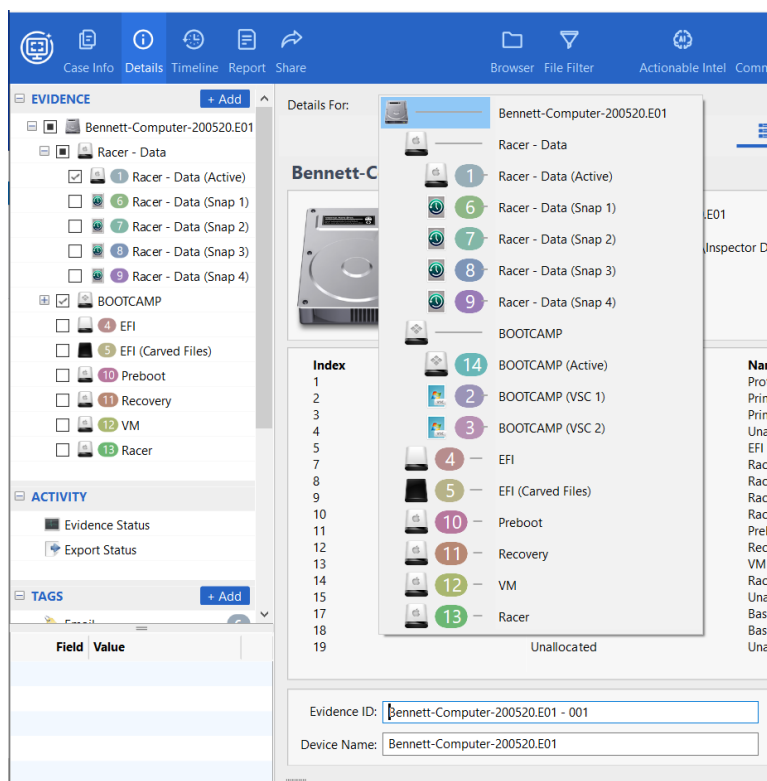
In the Component list to the right of Evidence, click **Add** to add another item to the case. To remove an item from the case, open the context menu and click **Remove <Name> from Case**.

To show or hide the Component list and File Information pane, click **Window > Hide Toolbar and Sidebar**.

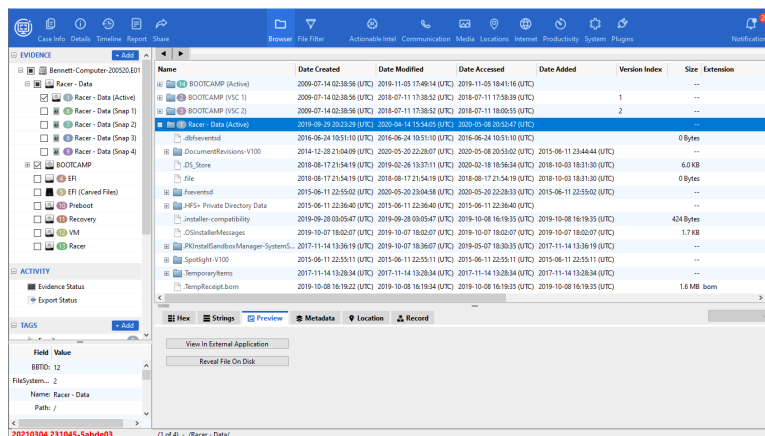
Each evidence item is associated with a colored badge number. The numbering is sequential and is assigned by Inspector upon the initial evidence ingestion. When an image that contains multiple volumes is added to Inspector, those volumes appear in the component pane with sequentially numbered badges. The image container itself is not numbered.



To see any data from a specific item within any Inspector view, mark the checkbox next to the appropriate volume. If the checkbox is not marked, that particular item will not appear in any view. The exception to this is the Details view, where each volume added to Inspector can be selected in the Details For field.



All the other views show data from the selected items. The Browser view shows the hierarchy of each volume along with the numbered badge and the volume label.



Likewise, the File Filter view shows the numbered badge in the first column for each corresponding item. All views within Inspector work this way.

If a volume is removed or added, badge numbering does not change to reflect the addition or removal. Any subsequently added volumes continue to be numbered incrementally.



## Activity

The Activity section of the Component list includes these categories.

- Export Status
- Evidence Status

## Export Status

In the Activity section of the Component list, click **Export Status**. File export progress indicators are displayed here. A numerical badge next to Export Status indicates how many files are currently exporting. Completed exports are also listed.

To clear the Export Status list, in the bottom left corner of the of the Content pane, click **Clear List**.

## Evidence Status

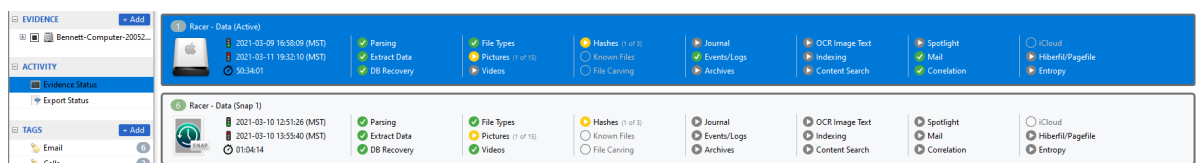
In the Activity section of the Component list, click **Evidence Status** to see the status of device acquisition and data processing, and to perform additional data processing on a device.

Each evidence item has its own area. All processing options are shown for the item with the status of each. File processing options may be activated at any time during an examination. To start a process that has not yet begun, click **Run** for that process.

You may run the Known Files and the File Carving processes multiple times. Click **Run** next to Known Files to calculate hash values again. Click **Rerun** in the File Carving column to locate and select additional file types in unallocated space.

**Note:** When you click **Rerun**, Inspector temporarily removes the device from the case in order to reprocess the data. Therefore, tags associated with data contained on the partition are permanently removed from the case.

**Note:** For devices with APFS, file carving must be done at initial ingestion. After media containing APFS is processed, the File Carving process is not available.





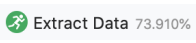







These are the available processing options.

Option	Description
Parsing	Analyzes the file system and file paths
Extract Data	Processes data to populate data in Actionable Intel, Communication, Locations, Internet, Productivity, and System tabs
DB Recovery	Recovers deleted entries from databases
File Types	Performs file signature analysis and compares the files' headers to the files' extensions
Pictures	Locates and builds thumbnails for all images, runs Image Analyzer
Videos	Locates and splits video files into sixteen frame sequences, runs Image Analyzer
Hashes	Calculates file hash values
Known Files	Compares file hashes to the selected hash databases
File Carving	Attempts to carve known file types from unallocated space
Journal	Process \$USNJRL file in Windows and macOS .fsevents
Events/Logs	Process Windows \$log analysis, EVT/EVTX analysis, macOS ASL logs, and macOS unified logs
Archives	Expands and processes the following archive files: zip, gz, 7z, tar, tar
OCR Image Text	<p>Process image (picture) files to extract text. Optical character recognition (OCR) converts text detected in the image into plain text which can be indexed and then searched. This process can be slow and is limited to these image types.</p> <ul style="list-style-type: none"> <li>• pdf</li> <li>• tiff</li> <li>• bmp</li> <li>• png</li> <li>• jpg</li> <li>• gif</li> </ul>
Indexing	Builds a smart index from data in allocated space
Content Search	Runs built-in searches against memory files
Spotlight	Process macOS Spotlight extended attribute data
Mail	Process Apple Mail, Outlook mail files
Correlation	Identifies correlated events done by the system, by a user, or by device.

Option	Description
iCloud	Process iCloud backups from iCloud production files
Hiberfil/Pagefile	Process Windows memory hibernation file and pagefile
Entropy	Determines possible encryption level of files

These are the possible status symbols that can appear for processing option.

Symbol	Meaning
	<p>Overall progress of partition processing for the selected processing options.</p> <p>Green light shows when processing started.</p> <p>Yellow light shows when processing is still in progress.</p> <p>Green light shows when processing completed.</p> <p>Timer shows the time it took to process the partition.</p>
	Seen when Parsing or DB Recovery processes are running.
	Process has completed.
	Process has completed, but there are more options to run that were not selected.
	Process is running, but not complete. The process cannot be paused.
	Process is waiting to run.
	Process is running, but not complete. The process can be paused.
	Process has not been chosen to run.
	Process cannot run on the partition.
	There was an error with the process.

With an evidence item selected, Inspector shows a full log of the processing options run on the selected evidence. When a process is running, a pie progress wheel will display next to the device in the Component list which is processing. The pie progress will show the percentage of completed items.

In the Component list next to the Evidence Status item, a numerical badge indicates the number of devices currently processing. A numerical badge with the number of processors running for a given device appears next to each device in the Component list. An examiner may not view any data while the badge on the imported device reads "Busy." The badge displays a number as soon as the parsing process is complete.

Once parsing is completed on a partition, the examiner can begin browsing data in various views, though it must be remembered that not all data is available to view until processing is complete.

When all the processors have completed, the case is fully ready for review, and an examiner may select any of the toolbar buttons to access different Inspector views.

Certain processes can be paused during their progress. These processes will be identified by the Pause button. When clicked, the processor halts its progress and displays the gray Run button. To resume processing, click **Run**.

The Hashes processor calculates MD5, SHA1, or SHA256 hash values (or any combination of the three) of the files within the selected evidence item. This processor can be rerun at a later date if the examiner wishes to recalculate the file hash values. To rerun this processor, click the yellow **Run** button in the Hashes column, and right click on the desired hash type in the Hash Types window that appears. A **Rerun** button appears. Click **Rerun** and the Complete status will change to a checkbox, which can be selected for processing.

**Note:** You may disconnect the Inspector dongle while importing and processing devices. The dongle must be connected to begin device acquisition and parsing, but you may then remove the dongle. The Dongle Required message appears and remains while the dongle is disconnected from the system, but processing continues in the background. You must reconnect the Inspector dongle to resume interacting with Inspector.

## Content Searches

The Content Searches section of the Component list allows users to create Content Searches and displays Content Searches that have been run. For more information, see [Search](#).

## Index Searches

The Index Searches section of the Component list provides access to the Smart Index. New queries of the Smart Index can be created, and saved queries can be accessed. For more information, see [Search](#)

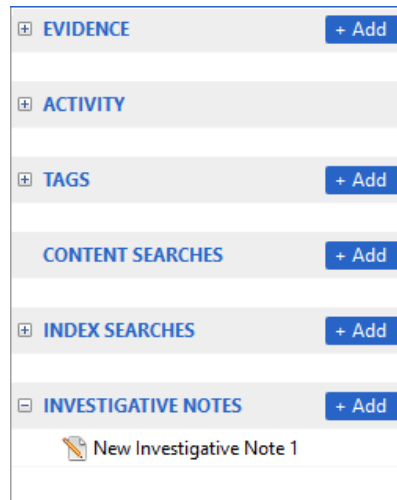
## Tags

Items tagged are accessible via Tags the Component list. For more information, see [Tags](#).

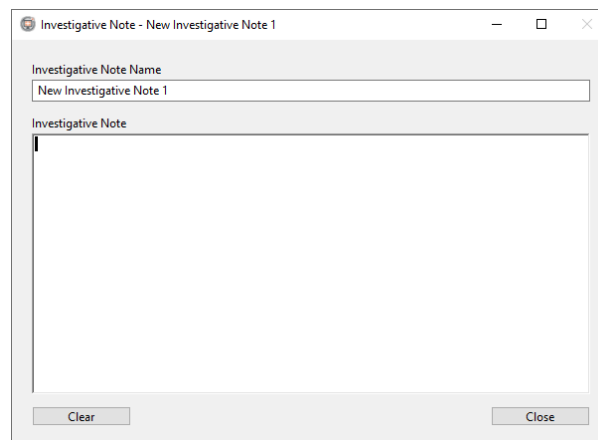
## Investigative Notes

Investigative Notes are accessible in the Component list. Investigative Notes provide an area for the examiner to copy and paste or type in information they wish to note during the analysis.

To add an Investigative Note, in the Component list click **Add** to the right of Investigative Notes.



In the Investigative Note window, you can name the note and then paste or type content. Investigative Notes are saved in the case file but cannot be put in the analysis report.



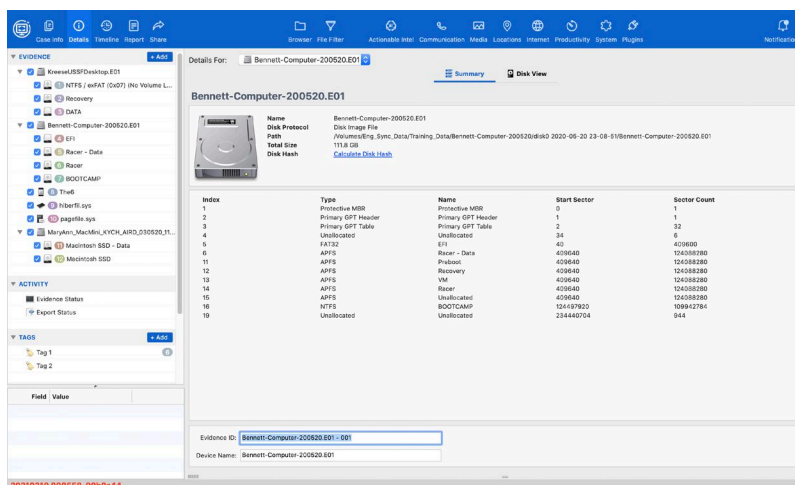
## Details View

In Inspector, the Details view shows information about the device, device partition, file, and folder for each evidence item in the case. Disk images display differently in the Details view depending on the type of item type (for example, partitions, unallocated space, folders, Android devices, and so forth). You can choose whether to include items shown in the Details view in the examiner report. For more information, see [Reporting](#).

In Details view, you can copy and paste text from the Content pane into a text file or export the text to a spreadsheet or database file. To the right of the device icon, select any or all of the device description text, then use your operating system's shortcut keys to copy and paste the text into your text file. To export the selected text items to a tab-delimited or CSV file, select text items in the Content pane, then open Inspector's context menu and click **Export Selected Rows**.

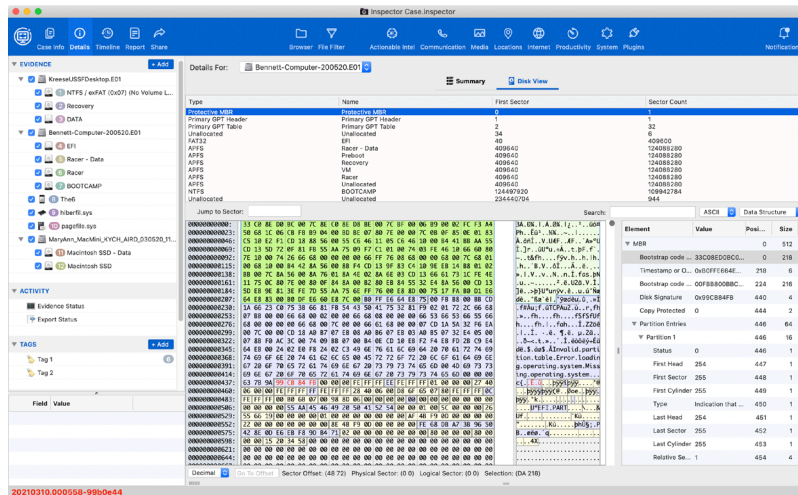
## Details View for Disk Images

In the Evidence section of the Component list, select a disk image. In the toolbar, click **Details**. The Summary tab in the Content pane displays image attributes such as the device name, disk protocol, disk path, total size and MD5, SHA1, and SHA-256 hash values (or a Calculate Disk Hash link if a hash has yet to be performed). Information about a partition is shown, such as partition type, partition name, start sector, and sector count, for boot record, free space, EFI, file system, etc.



The Summary tab offers a section at the bottom for entering an evidence ID and customizing the device name (Inspector automatically populates the Evidence Name text field, however this may be changed according to company/agency practices).

The Disk View tab offers a raw look into the disk structure itself. From this view, the full partition list is displayed as in the Summary view; however, each partition type may be selected to display the corresponding disk view. In addition, the Data Interpreter displays and interprets any desired highlighted text that is in the hex view.



It is also possible to search for strings or hex values from this view. In order to find a deleted HFS partition for example, the ASCII value of HSF can be entered into the search field. Press ENTER to start the search.

The first time a hit is found, it is highlighted in bright green. To find more occurrences, use these keyboard shortcuts.

- Mac computers: CMD+G
- Windows computers: CTRL+G

In Disk View, certain data structures for various filesystems are color coded, and you can review their interpreted values in the Data Structure view. For more information, see [Hex Templates and Data Structure View](#).

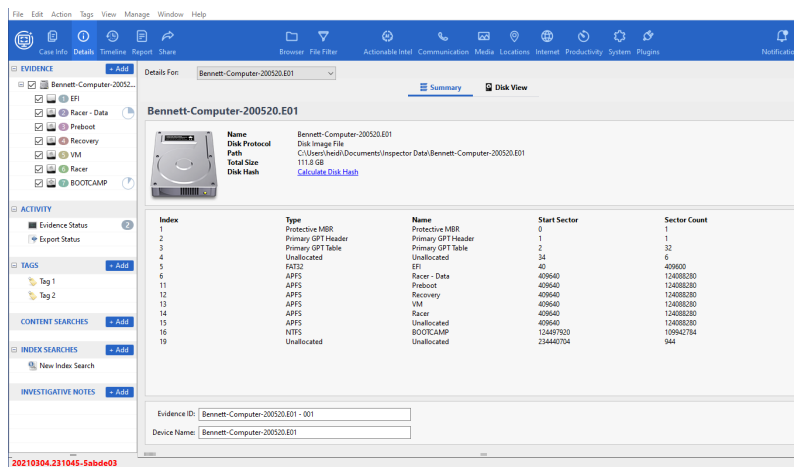
## Details View for Partitions and Imported Folders

In the Evidence section of the Component List, select a disk image partition or imported folder. In the toolbar, click **Details**.

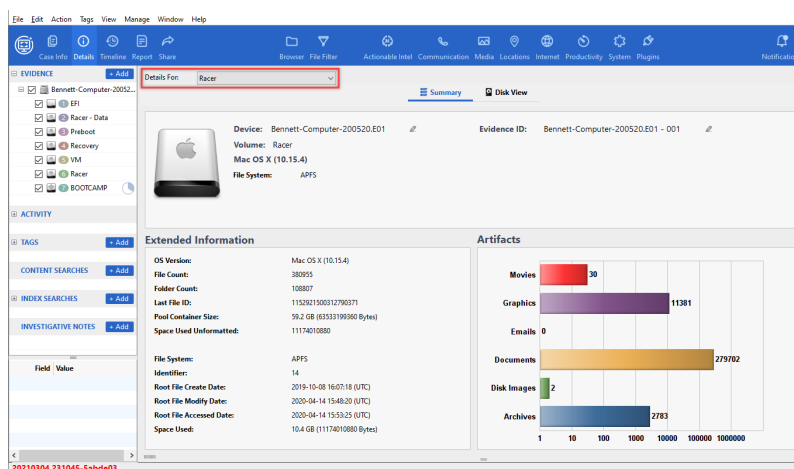
The Details view has two sub-views, Summary and Disk View.

## Summary View

The Summary view in the Content pane shows information about the top-level selected item, such as its name, disk protocol, total size, and index.



In the **Details For** field, choose a specific evidence item to see Extended Information and the Artifacts bar chart.

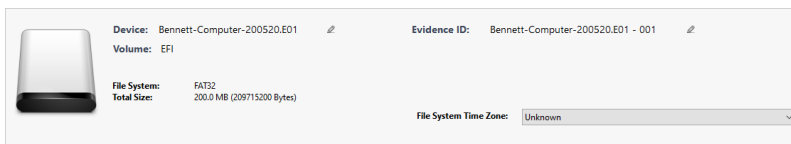


In Extended Information, you can see more details for the selected evidence item such as as file system type, total size, space used, space available, and timestamps for creation, modification, and access. For all standard volume types, Inspector parses out "Root File" timestamps that correspond to the root file within the volume.

To change the Device name or Evidence ID, click **Edit** (pencil icon) to the right of either field. Type the appropriate name in the **Device** field or the appropriate information in the **Evidence ID** field, and then click outside the text field to escape it.



For FAT16 and FAT32 volumes, you can select the time zone in the File System Time Zone field, above the Artifacts bar chart.



In the Artifacts bar chart, you can see the quantity of file types for items such as movies, graphics, emails, documents, disk images, and archives. Inspector automatically detects the presence of archive files (.zip, .sit, .tar) and disk image files.

When you double-click one of the colored bars, the File Filter view appears and shows the appropriate analysis view according to the selected bar.

## Disk View

To see the selected partition in its raw view, click **Disk View**. This lets you see and search any free space, along with slack space, within the partition. Only data from within the selected partition is seen in this view. To see data outside of the partition, you must select a different partition or the full disk in the Details For field.

To use the Disk View sub-view in other Inspector views, open the context menu for a selected item, and then click **Reveal File in Disk View** to see the first sector of the selected file in Disk View.

## Notes for macOS Computers

Information is also parsed from various macOS plist files including model, host name, serial number, macOS setup timestamp, time zone, language, AirPort ID or AirPort Discoverable Mode, and MAC and IP address.

For macOS 10.15, macOS information is parsed on the <System Volume> - Data partition, not the system partition (<System Volume>).

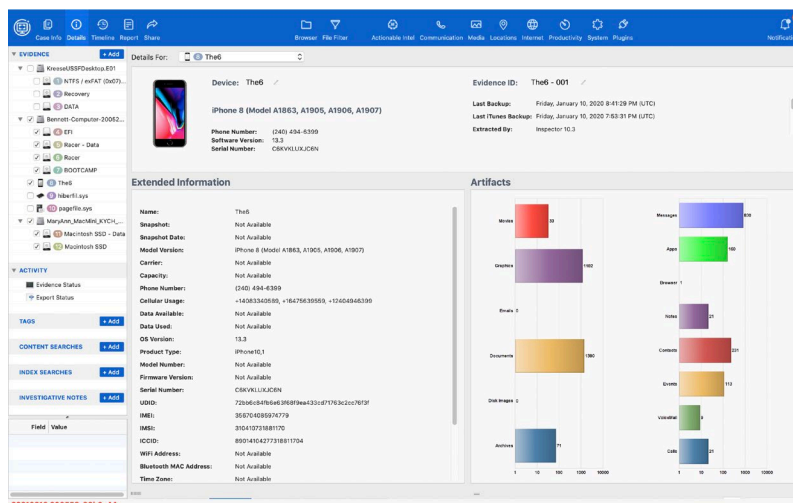
For HFS+ volumes, Inspector does not parse the file and folder counts from the volume header. Rather, it adds up the total number of files and folders based on what has been parsed from the catalog plus the raw HFS files.

The Volume Create Date timestamp for HFS+ volumes is stored in local time, based on the system's local time zone setting, rather than based on UTC. Inspector denotes this by showing (Local) next to the Volume Create Date timestamp. Volume timestamps for HFS+ volumes are parsed from the volume header.

## Details View for Mobile Devices

The Details view shows specific device information, including iOS device backup folder information for each iOS item in the case. Device items displayed in the Details view may also be included or excluded in the examiner report. For more information, see [Reporting](#).

In the Evidence section of the Component list, select an Android device, iOS device, or iOS backup folder. On the toolbar, click **Details**. When a device is selected in the Component list, the Content pane displays device attributes such as device type, OS version, phone number, cellular usage, serial number (when available), model number, UDID, AirDrop ID (iOS devices), AirDrop Discoverable Mode (iOS devices) and last iOS backup timestamp (iOS devices).



When an iOS backup folder is selected in the Component list, the Content pane displays attributes such as the backup folder's associated device type, iOS version, phone number, serial number, UDID, IMEI, AirDrop ID, and last backup timestamp display.

To change the Device name or Evidence ID, click just to the left of the pencil icon. Type the appropriate information into the text field and click outside the text field to escape it. The modified text appears.

In Artifacts, two bar graphs appear. Inspector automatically detects the presence of archive files (.zip, .sit, .tar) and disk image files. The left bar graph displays file counts by file type for these file types and others, such as graphics, documents, emails, movies, and disk images. The right bar graph displays file counts by file type for messages, apps, browser artifacts, notes, contacts, events, voicemail, and calls.

When you double-click on a colored graph bar, Inspector switches to and configures an appropriate analysis view depending on the item selected.

These are the options for the left bar graph.

Options	Description
Movies	Switches to File Filter view > Movie Files
Graphics	Switches to File Filter view > Graphics Files
Emails	Switches to File Filter view > Email Files
Documents	Switches to File Filter view > Document Files
Disk Images	Switches to File Filter view > Disk Image Files
Archives	Switches to File Filter view > Archive Files

These are the options for the right bar graph.

Options	Description
Messages	Switches to the Communication view, Messages sub-view
Apps	Switches to the System view, Applications sub-view
Browser	Switches to the Internet view
Notes	Switches to the Productivity view, Notes sub-view
Contacts	Switches to the Communication view, Contacts sub-view
Events	Switches to the Productivity view, Calendar sub-view
VoiceMail	Switches to the Communication view, Voicemail sub-view
Calls	Switches to the Communication view, Calls sub-view

## Details View for Other Types of Evidence Items

In the Evidence section of the Component list, select an evidence item (such as unallocated space [carved files], memory, folder, file, and so forth). On the toolbar, click **Details**.

The Artifacts bar graph shows file counts by file type for items such as movies, graphics, emails, documents, disk images, and archives. File count and bytes used are also shown. When you double-click on a colored graph bar, Inspector switches to and configures an appropriate analysis view depending on the item selected.

**Note:** You must run the unallocated space processors before all data can be displayed in the artifacts bar graphs. For more information, see [Managing Case Evidence](#).

## File Information Pane

All files contain metadata. Metadata is most easily defined as data about the data. Select a file in the Content pane. The file's metadata displays in the File Information pane.

If the selected file is a picture file, additional metadata or extended attributes such as hash values, date and time stamps, file paths, file size and EXIF, TIFF and location (GPS) data may be included in the file and displayed in the File Information pane. This screenshot shows metadata found in an image file.

While all file systems have some metadata in common, additional metadata is available for some file systems. Metadata for all file systems commonly includes:

- Name
- Path
- Size
- Extension
- Date Created
- Date Changed
- Date Modified
- Date Accessed
- Hash Values
- Location on Disk

Field	Value
BBTID:	171207
FileSystemID:	1697144
Name:	BMW_Infotainment.docx
Path:	/Users/josh/Documents/BMW_Ir
Size:	23003
SizeOnDisk:	23003
Extension:	docx
ContentExtension:	DOCX
Date Created:	2016-05-25 13:54:29 (UTC)
Date Changed:	2019-12-19 16:45:31 (UTC)
Date Modified:	2016-05-25 13:54:29 (UTC)
Date Accessed:	2017-08-04 16:01:00 (UTC)
FileSystemOffset:	UTC
fsType:	APFS
Directory:	No
Visible:	Yes
Locked:	No
Owner ID:	501
Group ID:	20
Permissions:	0644
Entropy:	0.
ForkCount:	1
Hash:1:SHA1:	84182125E865B4CB247B0F8B
Hash:1:SHA256:	754478A8302A804158DF21BEI
Hash:1:MD5:	E512CA75A0CBAADD0C40739!
Extents:	1
Sector Start:	38531152
Hash Set Category:	
Metadata	
BSD Flags:	0x40
com.apple.lastused...	833d1f5a0000000f50ea31b0
com.apple.macl:	010074cbef8bb5ef45cباد0875
Date Added:	2016-05-25 13:54:29 (UTC)
Tracked:	true
Spotlight	
kMDItemContentCre...	2016-05-25 13:54:29 (UTC)
kMDItemContentCre...	2016-05-25 00:00:00 (UTC)
kMDItemContentMo...	2016-05-25 13:54:29 (UTC)
kMDItemContentMo...	2016-05-25 00:00:00 (UTC)
kMDItemContentType:	org.openxmlformats.wordproce
kMDItemContentType...	org.openxmlformats.wordproce
kMDItemContentTyp...	org.openxmlformats.openxml
kMDItemContentTyp...	public.zip-archive
kMDItemContentTyp...	com.pkware.zip-archive
kMDItemContentTyp...	public.data
kMDItemContentTyp...	public.item
kMDItemContentTyp...	public.archive
kMDItemContentTyp...	public.composite-content
kMDItemContentTyp...	public.content
kMDItemDateAdded:	2016-05-25 13:54:29 (UTC)
kMDItemDateAdded...	2016-05-25 00:00:00 (UTC)
kMDItemDisplayName:	BMW_Infotainment.docx
kMDItemInteresting...	2017-11-29 00:00:00 (UTC)
kMDItemKind:	Microsoft Word 2007 document
kMDItemLastUsedD...	2017-11-29 23:06:43 (UTC)
kMDItemLastUsedD...	2017-11-29 00:00:00 (UTC)
kMDItemLogicalSize:	23003
kMDItemPhysicalSize:	24576
kMDItemUseCount:	3
kMDItemUsedDates[...	2017-11-29 05:00:00 (UTC)
kMDItemUsedDates[...	2017-11-29 08:00:00 (UTC)
kMDItemContentCh...	2016-05-25 13:54:29 (UTC)
kMDItemCreationD...	2016-05-25 13:54:29 (UTC)

## File System and Operating System Unique Metadata

Some metadata is unique to the file system. Metadata unique to APFS and HFS+ includes:

- Owner and Group ID
- Visible
- Locked
- Permissions
- Date Added
- Spotlight Metadata

Spotlight metadata includes a vast amount of information. Data can be filtered based on Spotlight metadata. For more information, see [Artifact Items](#).

HFS+ has additional metadata not found in APFS including:

- Label color
- Extended Attribute data

On Windows systems, Access Control Lists are stored in NTFS to control file system permissions. Each file on a Windows system has Access Control Entries (ACEs) to control file permission. The ACEs are parsed in File Information pane. For more information, see [Artifact Items](#).

## Media File Metadata

Picture and video files typically have additional metadata, including:

Category	Description
Summary	Image summary data (i.e., format, image dimensions, color space, aspect ratio, skin tone %)
TIFF	TIFF (originally standing for Tagged Image File Format) is a file format for storing images
EXIF	Exchangeable Image File Format. Includes GPS, camera make, model, settings and sound data
GPS	Location-based data stored by digital camera
Threat Category	Threat category calculated for the image file
Various other categories	Displays application-specific metadata

The metadata contained in each media file varies based on file type, how the media file was created, and other factors.

## File Content View

In the Content pane, select a file. If the File Content view is hidden, at the bottom of the Content pane select and drag the double hash marks up or down to view file data within the File Content view.

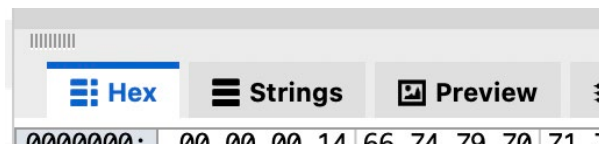
**Note:** The File Content view pane does not appear in the Details, Report, and Share views.

These are the tabs available in the File content view.

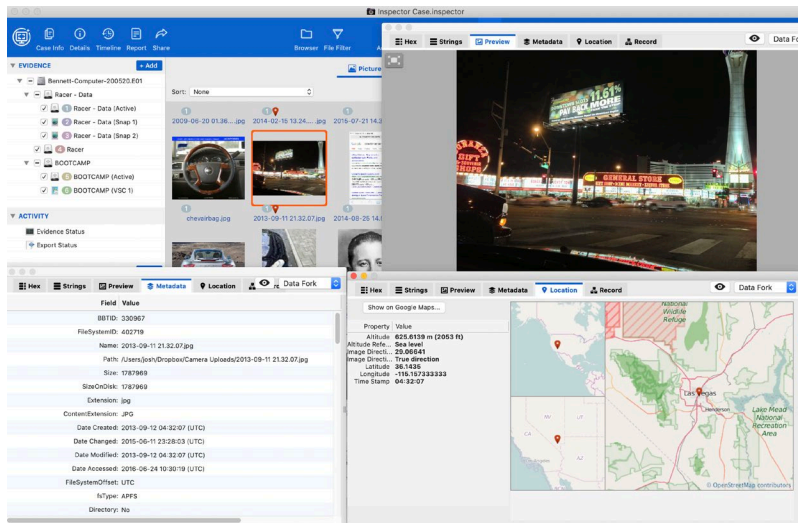
- [Hex](#)
- [Strings](#)
- [Preview](#)
- [Metadata](#)
  - [Location](#)
  - [Offline Maps](#)
- [Record](#)

You can "tear off" the File Content view as a separate window so you can simultaneously see multiple copies of the File Content view. This lets you see the File Content view in its own window.

In the upper left of the File Content view, immediately above the Hex tab, there is a grab handle appearing as several short, vertical lines. Click the handle and drag it away in any direction. A new File Content view window is created. This new window can be placed on another monitor if multiple monitors are being used, and it can be enlarged to the desired size.



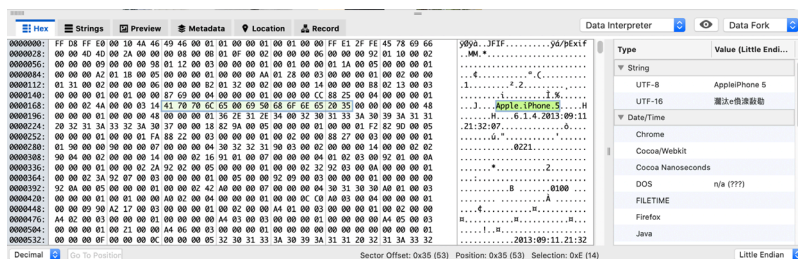
Additional tear-off File Content view windows can be created, and each one can be used to view different data if desired. For instance, one window may show the Preview tab, while another shows Metadata, and a third reveals Location maps. When a file is selected within the original case window, such as in Browser view, all of the tear-off windows update to reflect information related to that file.



There is no need to reconnect these tear-off windows to the original case window. Simply close each window when finished with it. Even though the File Content view can be hidden on the original case window, it is always there and never has to be reattached.

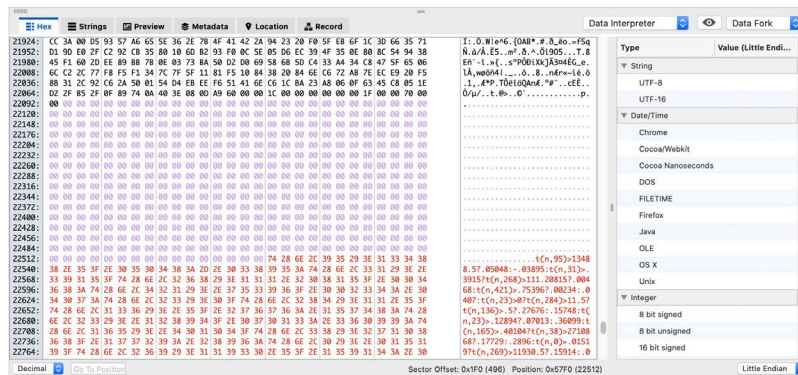
## Hex

Click **Hex** to display data in hexadecimal and ASCII characters. In the lower right corner of the File Content view, the sector offset, physical sector, logical sector, cluster start, and selection length for the current cursor position displays. Select and drag across data of interest to highlight it, open the context menu from the highlighted area, and then click **Tag Hex Data As** to tag the data and include it in the examiner report. For more information, see [Tagging](#).





When a file is examined in Hex view, Inspector displays allocated bytes of the file in black. The RAM slack (i.e., data from the last byte of the file to the end of the sector) is shown in a lavender color, and the disk slack (i.e., the start of the next sector to the end of the cluster [logical block on the Mac]) is displayed in red.



## Strings

Click **Strings** to display ASCII printable strings of three (3) characters or more. If the selected file is a text file, an examiner can perform a keyword search within the displayed text strings in both the Strings view and Preview views.

When the OCR (optical character recognition) process has completed, any text parsed from supported image file types can be seen on the Strings view. OCR text appears after this label: \*\*\*\*\* OCR Image Text \*\*\*\*\*. While you can search OCR text with an index search, a content search cannot find it because it does not exist as plain text. You may also use the OCR Image Text option in to filter image files that have recognized text.

When you click **Edit > Find**, A Find dialog box appears. You can drag search results to select and tag them.

## Preview

Click **Preview** to see a file as it would appear in its native application.

**Note:** Not all file types display in Preview view. Unicode text is not supported in Strings view.

You can toggle the preview between the default (scaled to fit the Preview tab) or actual size. The appearance of the toggle depends on the preview displayed at the moment.



In the upper right corner of the File Content view, click **View** to see data contained in a file's data fork, resource fork, and/or ADS (alternate data stream).

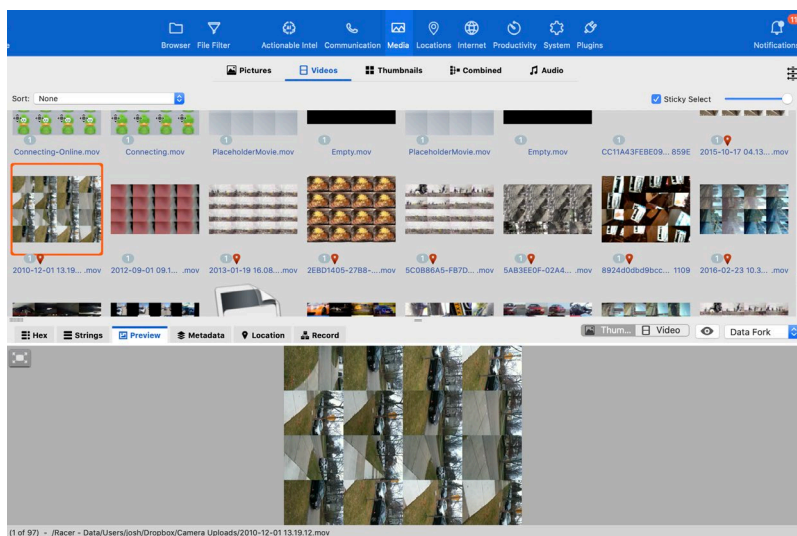
**Note:** Data Fork is the default view, as the data fork is where file data resides the majority of the time. However, file data on an HFS+ file system is sometimes stored in the resource fork. If a file has a resource fork, both Data Fork and Resource Fork view options are present in the drop-



down menu. Inspector looks to see if a file has a resource fork and if so, automatically adds this option to the drop-down menu. Likewise, if an NTFS file has data in an ADS, an option for viewing the ADS will be included in the drop-down menu.

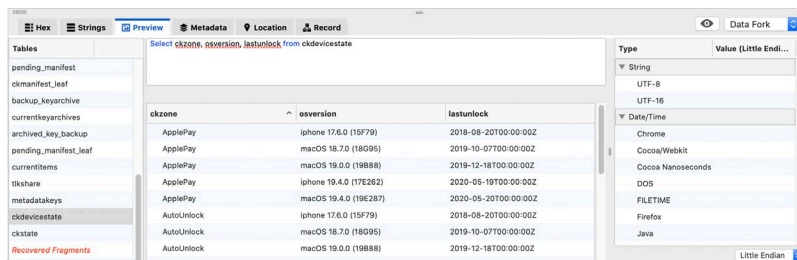
You can preview video files. To see the video file split into sixteen frame sequences and displayed as a 4 x 4 mosaic, at the top right of the File Content view, click **Thumbs**.

If you click **Video**, the video file is rendered with playback controls. To play the video, click **Play**.



In the Content pane, select a file and press the spacebar, or select the **Eye** button to view the file using Quick Look (Mac only). Quick Look displays native Apple application files (and some third-party application files) the same way a user sees them. Audio and video files play within the Quick Look view as well.

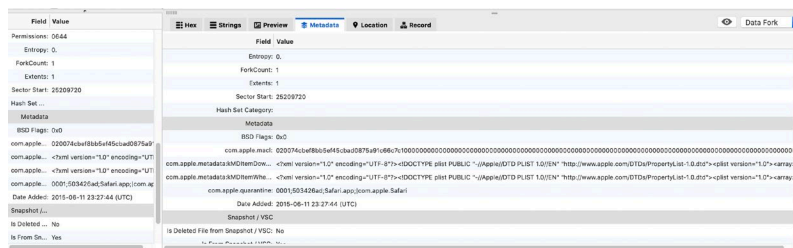
**Note:** The Quick Look feature works only when a Quick Look plug-in for the selected file type, or an application that supports the selected file type is installed on the forensic examiners analysis machine. Inspector allows for queries to be run on SQLite databases. Select a database and click **Preview** in the File Content view. Enter a valid SQLite query in the upper pane of the File Content view or double-click one of the database tables to the left. When the examiner double-clicks a table, a query is automatically populated. The query can be edited and run as desired, with results showing in the lower pane. When finished editing, press ENTER to run a query. Results can be exported as tab-delimited or CSV files. To do so, select the results and open the context menu, then select **Export Selected Rows** to choose the format and save location.



In the upper pane, known keywords (e.g., "SELECT" and "FROM") are displayed in **blue**. Inspector prevents processing of destructive user-defined SQLite queries (e.g., "CREATE" or "DELETE"). When typed, these destructive terms are displayed in **red**, and an error message is displayed. When an existing table or column name is partially typed and the cursor is placed anywhere within or directly after that partial name, the examiner can press TAB for autocomplete suggestions. A list of tables and columns that contain that partial name appears. The examiner can then select a table or column name from the list, and Inspector autocompletes the name in the query.

## Metadata

With any file selected, click **Metadata** in the File Content view. The metadata contents shown are identical to those displayed in the smaller File Information pane to the left, you can enlarge the pane as much as you need.



In some cases, only Hash:1:MD5 is shown as an available MD5 hash field; however, at other times additional MD5 hash fields may be shown. These numbers are related to the data fork, resource fork, and ADS fork.

- Hash:0 = mirror of data fork
- Hash:1 = data fork
- Hash:2 = resource fork (Mac)
- Hash:4 = ADS fork (Windows)

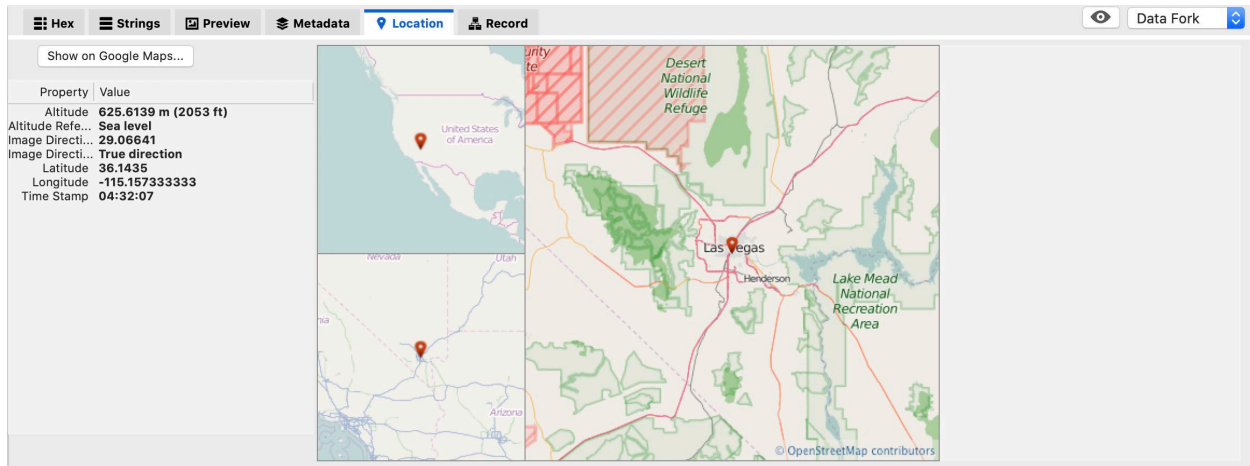
**Note:** A file can have more than one ADS fork, therefore MD5 hash number types can exceed 4. Inspector does not display a Hash:3.

## Location

Select any media file that contains geolocation (GPS) data (as indicated by a red placemark icon), or any applicable record in the Location view, then click **Location** in the File Content view to display one or more offline maps depicting the item's latitude and longitude coordinates. Inspector also displays a button to optionally view the location in Google Maps (if connected to the Internet), and other geolocation information contained in the file's metadata.

## Offline Maps

Inspector presents a set of static maps based on OpenStreetMap. Select a file that contains GPS coordinates and click **Location** in the File Content view. In the Location tab, you can see an offline map with three levels of zoom. You can download additional maps for additional zoom capabilities.



The zoom is currently set at levels 3, 5, and 8. When additional zoom level tiles are downloaded, Inspector increases its maximum zoom accordingly. When connected to the Internet, you may also zoom in by clicking **Show on Google Maps**. The default web browser opens to Google Maps, allowing control of the zoom level and viewing style. With Inspector, you can export files containing GPS information as a .kmz file or in .kml format. Select the files containing GPS data, open the context menu, click **Export > Export Selected Location Data As**, and then choose either KMZ or KML format. In the Export window, provide a file name, choose or create a destination folder, and then click **Export**. Inspector exports the GPS data to a .kmz or .kml file in the destination folder.

## Record

Select a file and click **Record** in the File Content view. The Record view displays the MFT record, catalog tree record, or FAT file system record for the selected file.

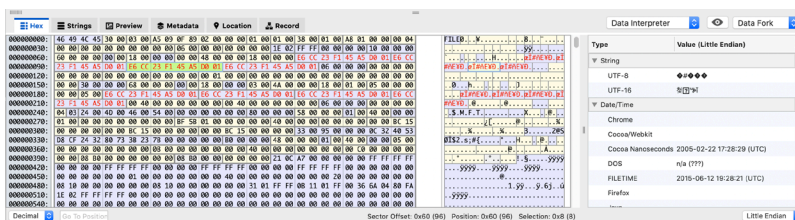
## Data Interpreter View

There is a hidden Data Interpreter view which can be slid into view from the right side of the File Content view. Select and drag the double hash marks left or right to view file data within the Data Interpreter. This view is hidden by default, but once opened it remains in the same position until you change it.

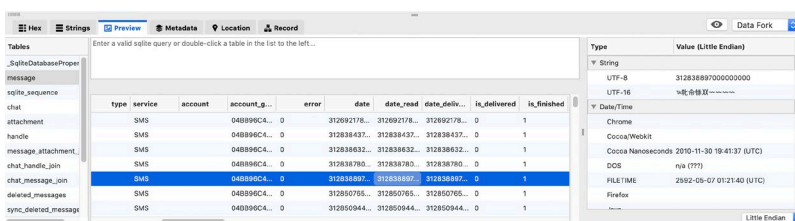
The Data Interpreter works when in the Hex and Strings views. It also works in the Preview view for certain file types such as databases and .plist. In the Hex view, select and drag across data of interest to highlight it. The Data Interpreter automatically update its display accordingly.

The interpreter has three modes in which the data may be displayed: Big Endian, Little Endian, and Both. Choose the option which best suits the data type that is being decoded or interpreted. Choosing Both allows both the Big Endian and Little Endian values to appear side by side. Use the disclosure triangles in the data type rows to show or hide values.

In this example, the date is highlighted in green. Looking at the Big Endian FILETIME date, it becomes clear that the date is not real; however, the Little Endian date is. This might lead the examiner to conclude that this is a Microsoft date, as Microsoft uses the Little Endian storage format for integers (most significant bit first).



**Note:** As the Data Interpreter view is expanded, the adjacent view decreases, which causes the highlighted data to move.



Values from within .plist files and databases can be selected for interpretation. Clicking on **Preview** while viewing a database file will display the database structure. Select the desired table at left to view its contents. Values stored as integers can be interpreted. Click on the value in the lower pane, and the Data Interpreter decodes it. For example, in the screenshot above, a date value (1308221028) within the highlighted row is clicked, and it is interpreted into all the values the Data Interpreter can decode.

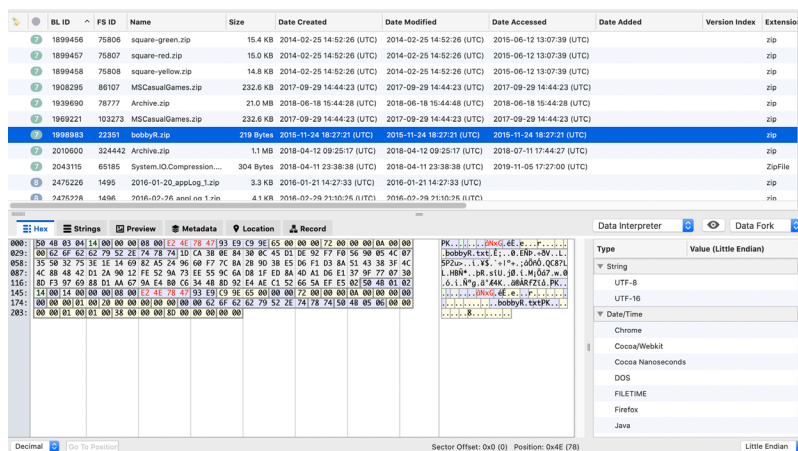
These are values decoded by the Data Interpreter view.

String	Date/Times	Integer	Floating	Other
UTF-8	Chrome	8 bit signed and unsigned	Single (4 byte)	Base64
UTF-16	DOS	16 bit signed and unsigned	Double (8 byte)	
	FILETIME	32 bit signed and unsigned		
	OS X	64 bit signed and unsigned		
	Cocoa/Webkit			
	Cocoa Nanoseconds			
	Unix			
	Firefox			
	Java			
	OLE			

The Data Interpreter view is also available within the Disk View, where the full evidence disk is presented in a raw form. For more information, see [Details View for Disk Images](#).

## Hex Templates and Data Structure View

Inspector can view binary data structures using templates. Templates can take the mystery out of binary data by allowing the data to be understood in an intuitive way. Rather than displaying the raw hex bytes of the file Inspector can show the file parsed into a hierarchical data structure for easy understanding. This goes beyond the Data Interpreter view to display arbitrary values of selected data.



Inspector will automatically apply a template to a file when the file is selected and a template for that file type exists.

The screenshot shows the Inspector application interface. The top pane displays a list of files with columns for BL ID, FS ID, Name, Size, Date Created, Date Modified, Date Accessed, Date Added, Version Index, and Extension. The bottom pane shows the Data Structure view for a selected ZIP file. The Data Structure view lists various elements with their values, positions, and sizes. The 'DOS Date & Time' element is highlighted, showing a value of 2016-11-24 09:55:04 (JUNK).

Element	Value	Position	Size
ZIP		0	
File Record [0]		0	
Signature	ZIP FILE RECORD (0x04034b50)	0	
Version Info		0	
Flag Type	None	6	
Compression Type	DEFLATE	8	
DOS Date & Time	2016-11-24 09:55:04 (JUNK)	10	
CRC	0x8C9E993	14	
Compressed Size	101	18	
Uncompressed Size	114	22	
File Name Length	10	26	

In the previous example, a zip archive file was selected and by choosing the Data Structure option, the zip file data structure is revealed. All the parts of the data structure from the template are shown to the user including the element name or variable, which is spelled out for the benefit of the user, the value of that item, the position from the beginning of the file and the size of the particular structure. This allows a deeper view into otherwise overlooked data structures. The template data returns a color coding for specific data types which can be chosen by the user as well as highlighting forensically important items such as dates and times, usernames, paths, etc.

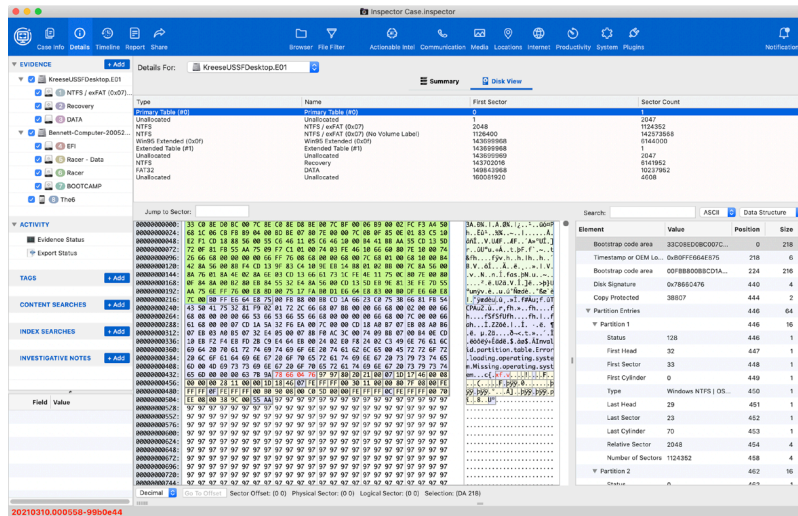
The data structure is made up of a series of variables and selecting a variable in the list shows which hex bytes correspond to that variable (in the image above, the variable DOS Date & Time corresponds to the hex bytes E2 4E 78 47 at position 10). Highlighting either the hex data or the variable will change the other component. In addition, the Data Interpreter view can be selected and the corresponding data will be displayed there as well.

The screenshot shows the Inspector application interface with the Data Interpreter view selected. The Data Interpreter view displays the value of the selected variable (DOS Date & Time) in a list of variables. The 'DOS Date & Time' variable is highlighted, showing a value of 2016-11-24 09:55:04 (777).

Type	Value (Little Endian)
String	
UTF-8	0x0
UTF-16	0x0
Data/Time	
Chrome	1601-01-01 00:19:59 (UTC)
Cocoa/Webkit	2038-12-31 02:07:30 (UTC)
Cocoa/Nanoseconds	
DOS	2016-11-24 09:55:04 (777)
FILETIME	
Firefox	1970-01-01 00:19:59 (UTC)
Java	1970-01-14 21:04:26 (UTC)
OLE	
OS X	1941-12-30 02:07:30 (UTC)
Unix	2007-12-31 02:07:30 (UTC)
Integer	
8 bit signed	-30
8 bit unsigned	226
16 bit signed	20194
16 bit unsigned	20194
32 bit signed	1199066850



Templates for ZIP, TAR, SQLite, BMP, JPG, GIF, PNG, AVI, MP4, and LNK files are included with Inspector as well as templates for parsing HFS Catalog Records, MFT Records, FAT32 Records, Partition Tables, and boot sectors. It is not difficult to write your own template for Inspector to use.



Templates are written in Python and are very flexible since they may include if, for, or while statements as well as functions or complex expressions. A template is executed as a program, starting from the first line of the file. Data from that file is passed in from Inspector as a stream object and can then be read by the python template which will return the data structure for display back to Inspector after the data stream has been parsed.

The templates that come with Inspector (compatible with Python 3.8.2) are not designed to be altered by the user. Rather, users can create their own templates and place them in the following locations.

- macOS: `/Users/<username>/Library/Application Support/CellebriteTech/Template Scripts/`
- Windows 10: `C:\Users\<username>\AppData\Roaming\CellebriteTech\Template Scripts`

The built-in templates can be overridden by user-based templates. Templates work based off of the extension of a file. In other words, the templates are named `<extension>_template.py` where extension is the extension of the file the template is parsing. For example, a file with a .png extension would use a template named `png_template.py`. The following example demonstrates a simple PNG template. This template is designed to parse the chunk structure of a PNG image file.

```

#!/usr/bin/python
# -*- coding: utf-8 -*-
"""
File: png_template.py
Author: Cellebrite
Version: 1.0
Purpose: Template for parsing PNG structures.

Category: Image
Signature ID: 89 50 4E 47 0D 0A 1A 0A // %PNG
History:
1.0 Cellebrite Initial release
"""
from bbt_framework import *

def analyse_stream(stream):
    #PNG Files are Big Endian
    stream.little_endian = False

    # read the first 8 bytes which are the PNG signature
    sig = ""
    try:
        sig = stream.read_bytes(8)
    except:
        pass

    if sig != b'\x89PNG\r\n\x1a\n':
        root = TemplateField( "Invalid PNG Data", 0, stream.length(), "" )
        return root

    #create root field for PNG
    root = TemplateField( "PNG", 0, stream.length(), "" )

    # create signature field and append to the root field
    signature = TemplateField( "Signature", 0, 8, sig )
    root.append(signature)

    # Loop through the chunks until we get to the end.
    try:
        while stream.position < stream.length():
            # Read the chunk length, type, data and a checksum
            chunk_start = stream.position
            chunk_length = stream.read_uint32()
            chunk_type = stream.read_utf_8( 4 )
            stream.position = stream.position + chunk_length # Just move the position
            rather than reading the data
            chunkCRC = stream.read_uint32()

            # Add a field for this chunk
            chunk = TemplateField( chunk_type, chunk_start, chunk_length + 12, "" ) #
            Add 12: 4 bytes each for length, type and CRC
            root.append(chunk)

            # Each chunk has 3 or 4 sub_fields: size, type, possible data and CRC
            # Add size sub_field
            chunk.append( TemplateField( "Chunk Size", chunk_start + 0, 4,
            chunk_length))
            # Add type sub_field

```



```

        chunk.append( TemplateField( "Chunk Type", chunk_start + 4, 4,
chunk_type))
        # Add data sub_field if it's non-zero
        if chunk_length != 0:
            chunk_data_field = TemplateField( "Chunk Data", chunk_start + 8,
chunk_length, b'' )
            chunk.append(chunk_data_field)
            # Add CRC sub_field
            chunk.append( TemplateField( "Chunk CRC", chunk_start + 8 + chunk_length ,
4, chunkCRC))

        if chunk_type == "CgBI":
            chunk.value = "iOS PNG"
        elif chunk_type == "IHDR":
            chunk.value = "Image Header"
            # Move the stream position back so we can read data
            stream.position = ( stream.position - chunk_length - 4 ) # 4 accounts
for CRC

            chunk_data_field.append(stream.read_uint32_template("Width"))
            chunk_data_field.append(stream.read_uint32_template("Height"))
            chunk_data_field.append(stream.read_uint8_template("Bit Depth"))
            chunk_data_field.append(stream.read_uint8_template("Color Type"))
            chunk_data_field.append(stream.read_uint8_template("Compression
Method"))
            chunk_data_field.append(stream.read_uint8_template("Filter Method"))
            chunk_data_field.append(stream.read_uint8_template("Interlace
Method"))

            # Reset the position to where it was
            stream.position = stream.position + 4

        elif chunk_type == "IDAT":
            chunk.value = "Image Data"
        elif chunk_type == "IEND":
            chunk.value = "Image Trailer"

    except:
        import logging
        logging.exception( "error")
        if TemplateField.last_append == None:
            root.append( TemplateField( "Invalid PNG Data", stream.length(), 0, ""
))

        else:
            lastValidPos = TemplateField.last_append.position +
TemplateField.last_append.size
            root.append( TemplateField( "Invalid PNG Data", lastValidPos,
stream.length() - lastValidPos, "" ))

    return root

def process( file_name = "" ):
    # create the stream
    stream = BBTStream(file_name)
    # analyze the stream
    root = analyse_stream(stream)
    # display the result
    root.display()

```

```
if not BBTFunctionsAvailable:
    process( "sample.png")
```

**Note:** Template scripts must import the **bbt\_framework** module.

There is currently one other module that can be included for assisting with dates and times. This can be accomplished by importing the **datetime\_helpers** module.

These are the basic template structure definitions.

- **stream** - The input stream (i.e. reading the file from position N, where N is either the start of the file or some positional offset)
  - **stream.position** The current location of the read in the stream
  - **stream.length()** The length of the entire input stream
- **Little Endian vs Big Endian** - Data is translated based on Little Endian by default. To translate based on Big Endian, add the following to the beginning of **def analyse\_stream(stream)**

```
stream.little_endian = False
```
- **root** - The root field for the Template view

Creating the root field is done by defining a new Field with the name root, which has the length set to the entire input stream:

- ```
root = TemplateField( "<NAME OF STRUCTURE>", 0, stream.length(), "" )
```
- **root.append(defined Field)** Appends a simple or complex field to the root field of the Template view
  - **return root** Returns all of root
  - **def analyse\_stream(stream)** Wrapper for the functions that analyze the input stream and render data for the Template view
  - **def process( file\_name = "" )** Wrapper for the function that runs **analyse\_stream** and displays the results within Inspector itself

**TemplateField** is defined as (name, position, size, value, significant=False).

- **name** = The name of the field that will be visible in Inspector in the Data Structure view itself
- **position** = The start byte based on the stream's current position (i.e. If the stream's current position is 0, and this value is set to 4, the start byte for this TemplateField will be byte number 4).
- **size** = The size in bytes of the defined object (depends on object type)
- **value** = The actual interpreted value of the data based on the position and size
- **significant** = Is this value forensically significant (Subjective)

## Object types

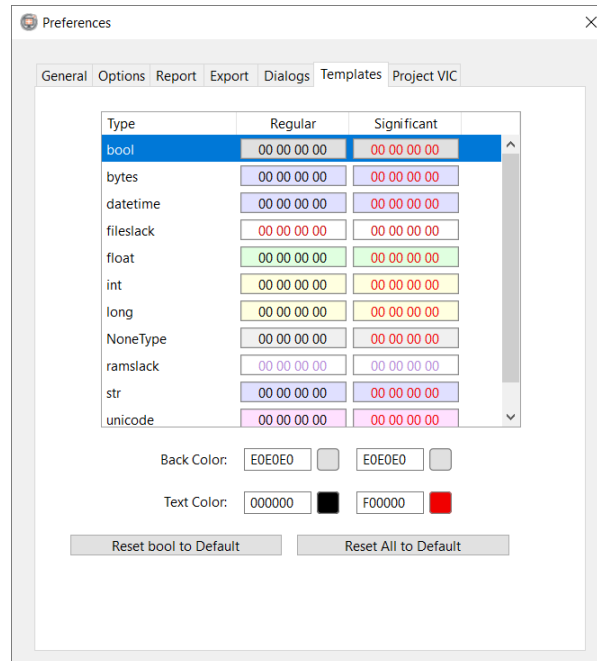
- **read\_bytes(self, count)** Read the input stream and return the bytes of that stream

**Note:** bytes that can be rendered in ASCII will be rendered; the rest will show their raw hex value.

- **read\_ascii(self, count)** Read the input stream and return the ASCII representation of that stream
- **read\_utf\_8(self, count)** Read the input stream and return a UTF 8 string representation of that stream
- **read\_string(self, count, encoding)** Read the input stream and return a string of the analyst's defined encoding
- **read\_string\_null\_terminated(self, encoding="")** Read the input stream and return a string based on a null terminator and of the analyst's defined encoding
- **read\_uint8(self)** Read the input stream and return an 8-bit unsigned integer
- **read\_int8(self)** Read the input stream and return an 8-bit signed integer
- **read\_uint8\_template(self, name, significant=False)** Read the input stream for an unsigned 8 bit integer and return a templatefield (Preferred method for getting a value as it tracks the position for you)
- **read\_int8\_template(self, name, significant=False)** Read the input stream for an signed 8 bit integer and return a templatefield
- **read\_uint16(self)** Read the input stream and return a 16-bit unsigned integer
- **read\_int16(self)** Read the input stream and return a 16-bit signed integer
- **read\_uint16\_template(self, name, significant=False)** Read the input stream for an unsigned 16 bit integer and return a templatefield (Preferred method for getting a value as it tracks the position for you)
- **read\_int16\_template(self, name, significant=False)** Read the input stream for an signed 16 bit integer and return a templatefield
- **read\_uint32(self)** Read the input stream and return a 32-bit unsigned integer
- **read\_int32(self)** Read the input stream and return a 32-bit signed integer
- **read\_uint32\_template(self, name, significant=False)** Read the input stream for an unsigned 32 bit integer and return a templatefield (Preferred method for getting a value as it tracks the position for you)
- **read\_int32\_template(self, name, significant=False)** Read the input stream for an signed 32 bit integer and return a templatefield
- **read\_uint64(self)** Read the input stream and return a 64-bit unsigned integer
- **read\_int64(self)** Read the input stream and return a 64-bit signed integer
- **read\_uint64\_template(self, name, significant=False)** Read the input stream for an unsigned 64 bit integer and return a templatefield (Preferred method for getting a value as it tracks the position for you)
- **read\_int64\_template(self, name, significant=False)** Read the input stream for an signed 64 bit integer and return a templatefield
- **read\_bool(self)** Read the input stream and return a boolean
- **read\_single(self)** Read the input stream and return a single float
- **read\_double(self)** Read the input stream and return a double float
- **read\_dos\_date\_template(self, name, swapBytes, tz\_offset\_minutes, tz\_unknown=False, significant=False)** Return the dos date and time from a 4 byte input stream which defaults to an unknown timezone since dos dates are local.

- `read_win_filetime_template(self, name, tz_offset_minutes, tz_unknown=False, significant=False)` Return the FILETIME from a 8 byte input stream.
- `read_mac_date_template(self, name, tz_offset_minutes, tz_unknown=False, significant=False)` Return the Mac OS Date and Time from a 4 byte input stream
- `read_unix_date_template(self, name, tz_offset_minutes, tz_unknown=False, significant=False)` Return the Unix Date and Time from a 4 byte input stream

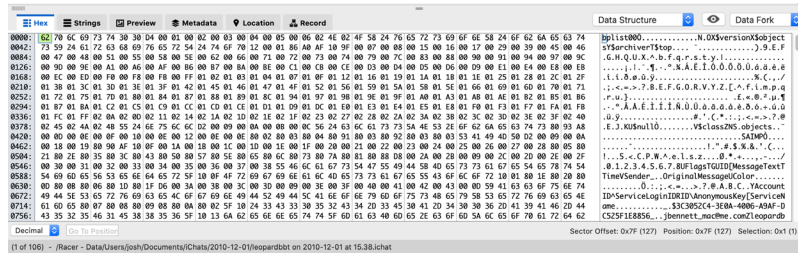
You can change the template colors in Inspector on the Templates tab in the Preferences. For more information, see [Inspector Preferences or Options](#).



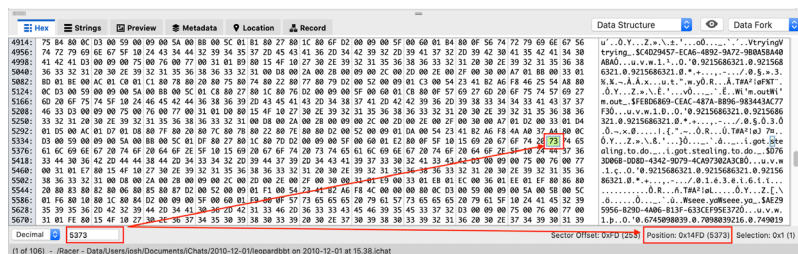
The standard data type colors which are returned by the template can be changed in this view. Highlight the datatype that needs to be changed and choose the back color and/or the text color to be altered. If the color block is selected a standard OS color picker will be displayed for color selection. Hex color values can also be entered manually within the text blocks. If a color needs to be reset to the default value for a single item, select that item and click **Reset <type> to Default** where <type> is the selected data type. To reset the entire color scheme to the default, click **Reset All to Default**.

## Go to Position in Hex View

The hex view has a position jump feature that allows the ability to move to a specific position (offset) within a file. There are three ways to change the position. The first and easiest is to use the Go to Position field on the bottom of the Hex tab view. The other two ways are through either the context menu or the **Edit**. Either of these will have the **Jump to Hex Offset** option, to let you enter a position to move to.



Type the position to jump to in the Position box, and Inspector shifts the position highlight to the numbered position. If a position is entered which does not exist, then Inspector highlights the last possible position to indicate there are no more positions to see. You can select whether to enter the position in decimal or hexadecimal notation.



## Recovered SQLite Records

Inspector attempts to recover deleted records from SQLite databases automatically. If a view exists for a specific SQLite database, such as the Messages sub-view, then any full, intact, or recovered records will be displayed in the Content pane. Recovered records are highlighted in red italics, denoting that they were at one time deleted records that have now been recovered.

Many partial items can also be recovered from SQLite databases. These partial fragments can be seen in the File Content view under the Preview tab. An SQLite database must be selected, and when you click **Preview**, the tables for the SQLite database display along with a table named Recovered Fragments.

The Recovered Fragments table is not part of the SQLite database. It is designed to display any recovered fragment data that cannot be placed into specific cells or columns, as there is no context for where the fragments originally existed. Like text items, these fragments can be tagged and placed into the report. When tagged, the tag icon appears next to the selected items.

**Note:** When the SQLite database is chosen from within any view, it will go through the recovery code to display the partial fragments. Sometimes this can take a small amount of time in which there will be little to no feedback, and it may appear that the Recovered Fragments table does

not exist. If no feedback occurs, either there are no recoverable items, or the recovery code is still running. For views which are normalized and have been pre-processed (such as Messages, Call, Contacts), the Recovered Fragments table is available immediately.

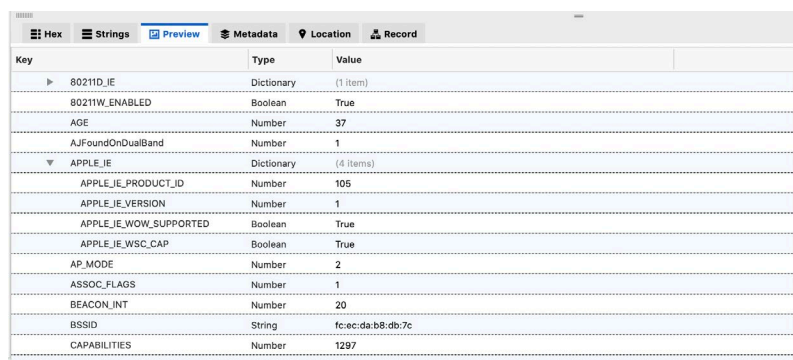
## Viewing Embedded .plist Data and .jpg Pictures

When a .plist contains embedded .plist data, you can see that data in the File Content view. Select a .plist that contains embedded .plist data, and click **Preview** in the File Content view. Embedded .plist data is denoted in the Type column. You can expand items to reveal .plist data.

- On a Mac computer, click the disclosure triangle.
- On a Windows computer, click +.

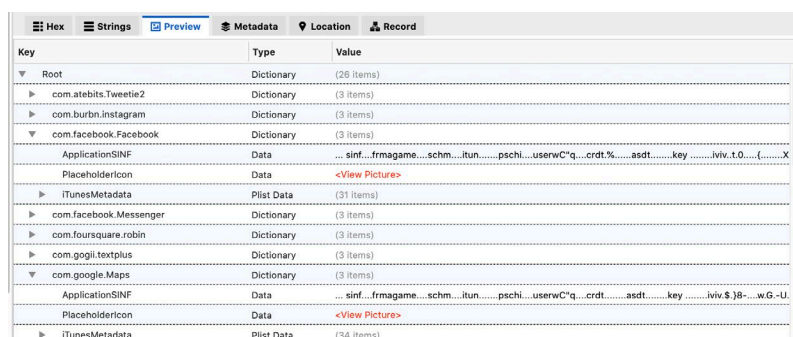
You can also expand all data within the .plist.

- On a Mac computer, press OPT while you click the disclosure triangle to the left of **Root**.
- On a Windows computer, press ALT while you click + to the left of **Root**.



| Key                    | Type       | Value             |
|------------------------|------------|-------------------|
| ▶ 80211D_IE            | Dictionary | (1 item)          |
| 80211W_ENABLED         | Boolean    | True              |
| AGE                    | Number     | 37                |
| AJFoundOnDualBand      | Number     | 1                 |
| ▼ APPLE_IE             | Dictionary | (4 items)         |
| APPLE_IE_PRODUCT_ID    | Number     | 105               |
| APPLE_IE_VERSION       | Number     | 1                 |
| APPLE_IE_WOW_SUPPORTED | Boolean    | True              |
| APPLE_IE_WSC_CAP       | Boolean    | True              |
| AP_MODE                | Number     | 2                 |
| ASSOC_FLAGS            | Number     | 1                 |
| BEACON_INT             | Number     | 20                |
| BSSID                  | String     | fc:ec:da:b8:db:7c |
| CAPABILITIES           | Number     | 1297              |

You can also see .jpg files that are embedded in a .plist. Click **<View Picture>** in the Value column, and the embedded .jpg opens in a new Plist Picture window.



| Key                      | Type       | Value                                                                                              |
|--------------------------|------------|----------------------------------------------------------------------------------------------------|
| ▼ Root                   | Dictionary | (26 items)                                                                                         |
| ▶ com.atebits.Tweetie2   | Dictionary | (3 items)                                                                                          |
| ▶ com.burtn.instagram    | Dictionary | (3 items)                                                                                          |
| ▼ com.facebook.Facebook  | Dictionary | (3 items)                                                                                          |
| ApplicationSINF          | Data       | ...sinf...frmagame...schm...itun...pschi...userwC"q...crdt...%...asdt...key...iviv.t.0...{...X     |
| PlaceholderIcon          | Data       | <View Picture>                                                                                     |
| ▶ iTunesMetadata         | Plist Data | (31 items)                                                                                         |
| ▶ com.facebook.Messenger | Dictionary | (3 items)                                                                                          |
| ▶ com.foursquare.robin   | Dictionary | (3 items)                                                                                          |
| ▶ com.gogii.textplus     | Dictionary | (3 items)                                                                                          |
| ▼ com.google.Maps        | Dictionary | (3 items)                                                                                          |
| ApplicationSINF          | Data       | ...sinf...frmagame...schm...itun...pschi...userwC"q...crdt...%...asdt...key...iviv.\$j8-...w.G.-U. |
| PlaceholderIcon          | Data       | <View Picture>                                                                                     |
| ▶ iTunesMetadata         | Plist Data | (34 items)                                                                                         |

When a database contains .plist data, you can see that data. In the File Content view select a database that contains .plist data and click **Preview**. Select a table in the left side, and then click **<View Plist>** to the right. A separate Database Plist window appears where you can also show or hide .plist data.

The screenshot shows the 'Preview' tab in the Inspector application. On the left, a list of tables is visible, including 'chat', 'message', and 'sync\_deleted\_message'. The main area displays a table with columns: ROWID, guid, style, state, account\_id, properties, chat\_iden..., service\_n..., room\_name, and account\_id. The table contains 10 rows of data, with some cells containing links like '<View Plist>'.

| ROWID | guid             | style | state | account_id  | properties   | chat_iden...    | service_n... | room_name    | account_id |
|-------|------------------|-------|-------|-------------|--------------|-----------------|--------------|--------------|------------|
| 1     | iMessage;+140... | 45    | 3     | 0451CB3B... | <View Plist> | +14083917...    | iMessage     | Ejbenne...   |            |
| 2     | SMS;+140...      | 45    | 3     | 5FE82478... | <View Plist> | +14083917...    | SMS          | E:           |            |
| 3     | iMessage;+140... | 45    | 3     | 0451CB3B... | <View Plist> | donniea01...    | iMessage     | Ejbenne...   |            |
| 4     | iMessage;+140... | 45    | 3     | 0451CB3B... | <View Plist> | godzillin@ic... | iMessage     | Ejbenne...   |            |
| 5     | iMessage;+140... | 45    | 3     | 0451CB3B... | <View Plist> | +12404946...    | iMessage     | Ejbenne...   |            |
| 6     | iMessage;+140... | 45    | 3     | 0451CB3B... | <View Plist> | bobby.rodr...   | iMessage     | Ejbenne...   |            |
| 7     | AIM;+140...      | 45    | 3     | 3C3052C4... | <View Plist> | g.fault         | AIM          | jbennett...  |            |
| 8     | SMS;+140...      | 45    | 3     | 5FE82478... | <View Plist> | 50472           | SMS          | E:           |            |
| 9     | iMessage;+140... | 43    | 3     | 0451CB3B... | <View Plist> | chat95331...    | iMessage     | chat95331... | Ejbenne... |
| 10    | iMessage;+140... | 45    | 3     | 0451CB3B... | <View Plist> | +14082500...    | iMessage     | Ejbenne...   |            |

You can also see .jpg files that are embedded in a database. In the File Content view, select a database that contains a .jpg file and click **Preview**. Select a table in the left and click **<View Picture>** to the right. The .jpg opens in a new Database Picture window.

## Managing List Views

Inspector allows for secondary sorting of columns. In most views that contain columns, clicking on a column header toggles between sorting by that column in ascending or descending order. A single arrow in the column header denotes a primary sort, as well as indicating the direction (up for ascending or down for descending).

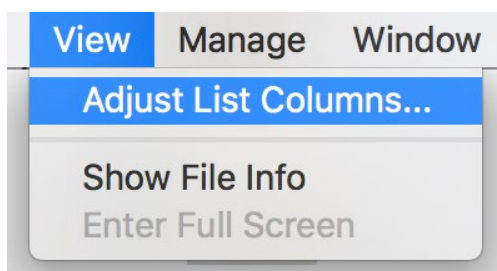
You can add a secondary sort by pressing SHIFT while you click a second column header. A set of double arrows are shown to denote a secondary sort. You can remove a secondary sort by clicking a column of choice for primary sorting.

The screenshot shows a table with two columns: 'Date Created' and 'Date Modified'. Both columns have sorting arrows. 'Date Created' has a single upward arrow (^), indicating it is the primary sort. 'Date Modified' has a double upward arrow (^^), indicating it is a secondary sort. The table contains three rows of data.

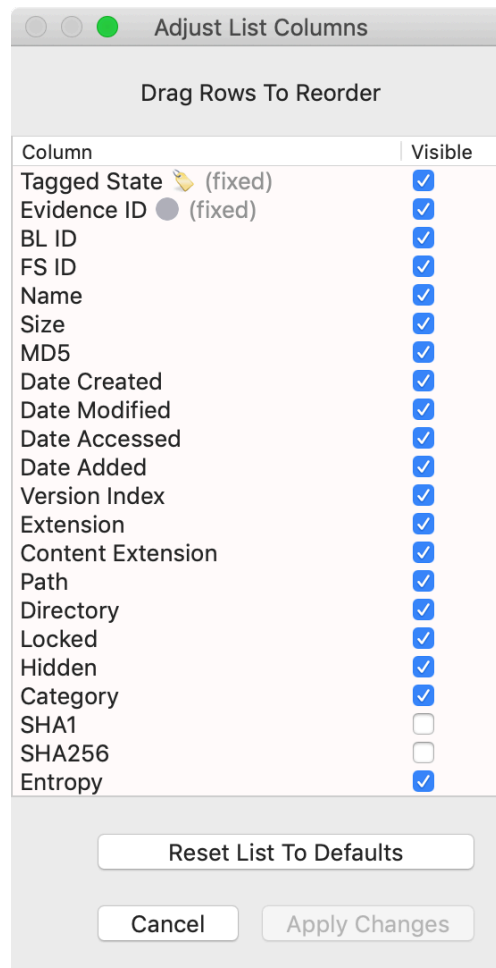
| Date Created ^   | Date Modified ^^ |
|------------------|------------------|
| 2014-10-01 (UTC) | 2014-10-01 (UTC) |
| 2014-12-27 (UTC) | 2014-12-27 (UTC) |
| 2014-12-28 (UTC) | 2014-12-28 (UTC) |

## Column Reordering

You can reorder columns by clicking **View > Adjust List Columns**.



A separate window opens. Select and drag each item in the list to the appropriate order. Each item can also be shown or hidden by activating or deactivating its checkbox in this list. When you have finished making changes, click **Apply Changes**. The columns now appear in the specified order.



To return columns to the default appearance, click **View > Adjust List Columns**, click **Reset List to Defaults**, and then click **Apply Changes**.



## Settings, Preferences, and Options

Inspector displays date, time and numeric attributes according to the settings for the operating system on the analysis computer. These settings determine how Inspector displays information in various views, as well as how some data is reported. It is important that these settings are appropriate for any given case.

Separately from that, you can manage preferences and options within Inspector itself.

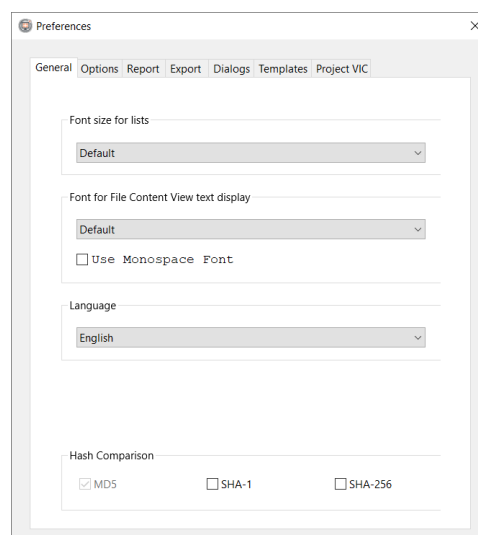
- [Inspector Preferences or Options](#)
- [System Preferences on Mac Computers](#)
- [System Settings on Windows 10 Computers](#)

### Inspector Preferences or Options

You can manage preferences and options for Inspector such as the default evidence list font size, iOS device deleted record recovery behavior, examiner report appearance, data export options, and search options. These are different from preferences or options for your operating system.

- In the menu bar for a Mac computer, click **Inspector > Preferences**.
- In the menu bar for a Windows computer, click **Edit > Options**.

The Preferences window appears.

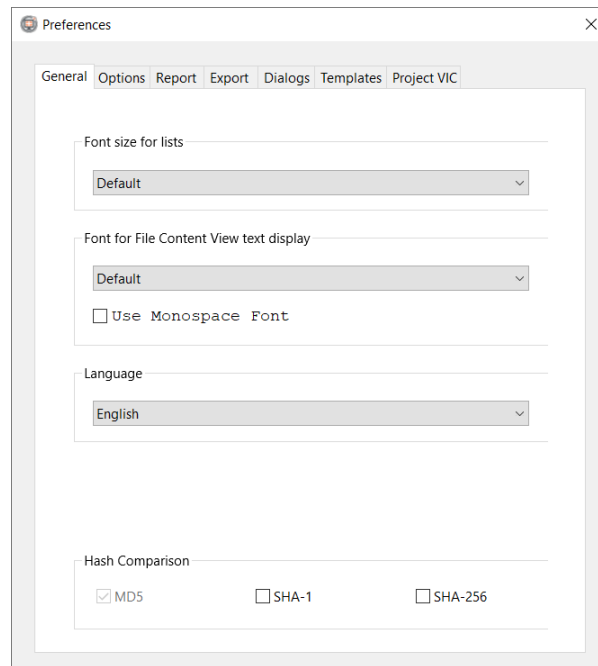


These are the tabs on the Preferences window.

- [General Tab](#)
- [Options Tab](#)
- [Report Tab](#)
- [Export Tab](#)
- [Dialogs Tab](#)
- [Templates Tab](#)
- [Project VIC Tab](#)

## General Tab

On the Preferences window, click **General**.



In the **Font size for lists** field, you can increase or decrease the default font size for lists in Inspector. This setting affects several views of the Content pane. It does not change data export font settings or font settings in data views that do not display data as a file list.

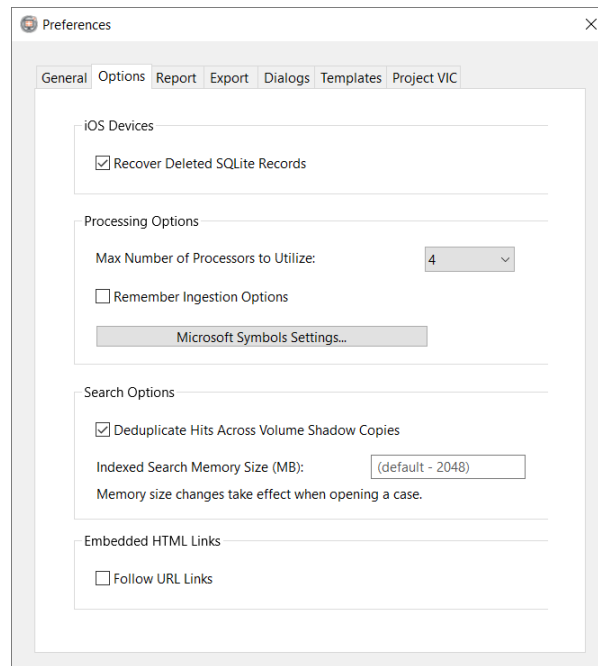
In the General tab, you can also change the font size for the File Content view and change the language.

Full Disk Access is a security feature in versions of macOS 10.14 (Mojave) and higher. It must be enabled for Inspector to function properly on Mac computers. When Full Disk Access is enabled, it is shown in the General tab. If it is disabled, you can click **Enable Full Disk Access**.

The General tab also provides options for **Hash Comparison**. Hash sets in Inspector can contain one or all of MD5, SHA-1 and SHA-256 hash values. By default, Inspector performs hash comparisons using MD5. You can mark the checkboxes for **SHA-1** and **SHA-256** to allow Inspector to perform hash comparisons using those hash values.

## Options Tab

On the Preferences window, click **Options**.



You can mark or unmark the **Recover Deleted SQLite Records** checkbox. Marking this box allows Inspector to automatically recover deleted iOS records from SQLite databases. The **iOS Recover Deleted SQLite Records** checkbox should remain marked unless problems occur while running Inspector.

## Processing Options

Inspector takes full advantage of machines with multi-core CPUs during device acquisition and searching. To manually set the maximum number of processors for Inspector to use, in the **Max Number of Processors to Utilize** field, choose a processor number. This change is effective for future ingestion, parsing, and searching. To make this change effective immediately, restart Inspector.

Mark the checkbox for **Remember Processing Options** if appropriate. When this option is marked, you can select custom ingestion options for a specific attached device (in the right portion of the Add Evidence window), cancel and close the case, then later reopen the case to find the processing options have been remembered in the Add Evidence window.

For information about Microsoft Symbols Settings, see [Adding a Memory File](#).

## Search Options

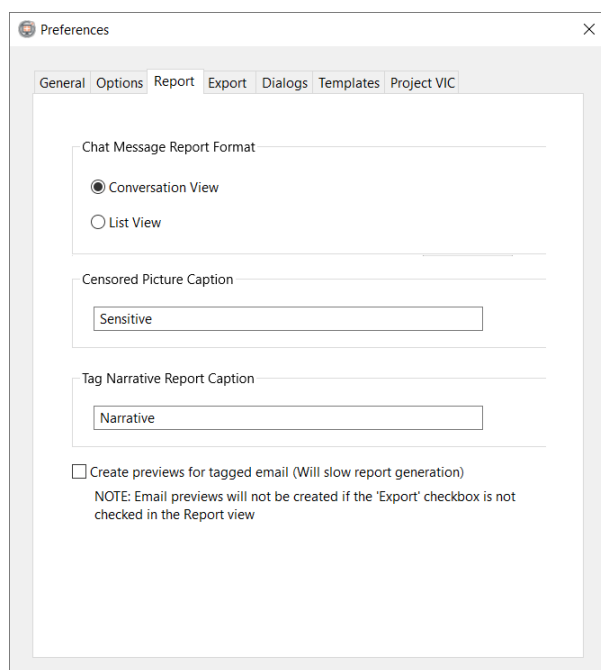
This section contains options for both Content searches and Index searches. The Deduplicate Hits Across Volume Shadow Copies option applies to Content keyword searches. For more information, see [Content Keyword Searches](#).

The Indexed Search Memory Size (MB) option relates to the amount of memory allocated to use by Inspector for indexing and index searches. The default setting allocates 2 GB (2048 MB) but can be increased or decreased. The minimum is 512 MB, the maximum is 100 GB. When Index Search Memory Size (MB) is changed, Inspector must be restarted for the new settings to take effect. Keep in mind, changing how much memory is allocated for Inspector may affect the overall performance of Inspector and any other software you are running on your system. Running Inspector processing options separately enhances performance.

In the Embedded HTML Links section, you can mark or unmark the checkbox to **Follow URL Links**.

## Report Tab

On the Preferences window, click **Report**.



You can choose the way SMS/MMS (chat) messages appear in the examiner report. The chat format preference has two settings.

- Select **Conversation View** to display chats in the examiner report the same way they appear natively on an iOS or Android device screen.
- Select **List View** to display chats in a list format.

**Note:** When generating a report in .docx format, if the report includes 5000 or more messages in the Conversation View, the report only shows messages in List View.

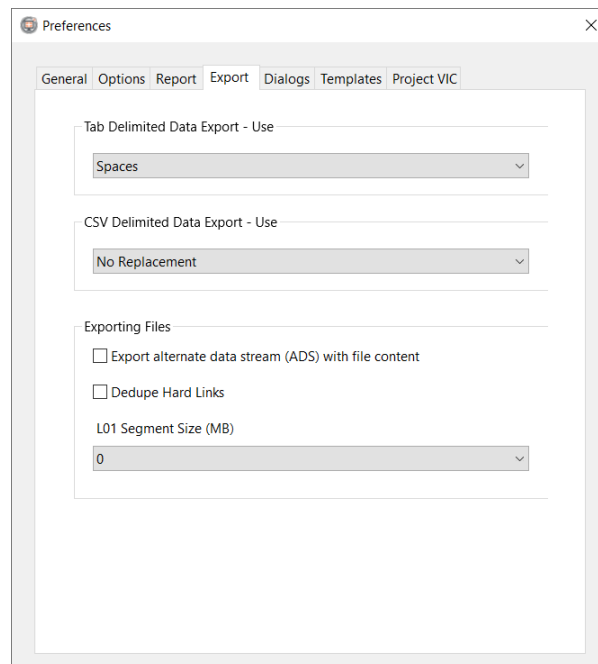
To customize censored picture captions and tag narrative captions, type the desired caption text into the **Censored Picture Caption** and **Tag Narrative Report Caption** fields respectively.

To enable email previews within reports, mark the **Create previews for tagged email (Will slow report generation)** checkbox.

**Note:** You must also mark the **Export** checkbox in the Report view and tag email within the Email sub-view of the Communications view or from Index Search when the **Type** field is **Email**. Email tagged in any other view, such as File Filter or in search results, does not result in previews in a report.

## Export Tab

On the Preferences window, click **Export**.



You can specify default file export settings. You can select and export data from the Content pane to a delimited text file, but this process requires some preliminary data manipulation. If a data cell contains non-printing characters (tabs, carriage returns, or line feeds), a clean tab or line-delimited export fails unless these characters are replaced or "escaped" prior to export.

For a tab-delimited data export, these are the available data export settings.

| Option |                        | Description                                                                                                                                                                       | Tab Delimited | CSV Delimited |
|--------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------|
| 1      | Spaces                 | Replaces all non-printing characters with spaces                                                                                                                                  | ✓             | ✓             |
| 2      | Escaped with \t and \r | Replaces tabs with \t<br>Replaces both carriage returns and line feeds with \r                                                                                                    | ✓             | ✓             |
| 3      | <TAB>, <EOL>           | Replaces tabs with <TAB><br>Replaces both carriage returns and line feeds with <EOL>                                                                                              | ✓             | ✓             |
| 4      | <TAB>, <CR>, <LF>      | This option treats both types of end-of-line characters as separate entities.<br>Replaces tabs with <TAB><br>Replaces carriage returns with <CR><br>Replaces line feeds with <LF> | ✓             | ✓             |
| 5      | No Replacement         | Does not replace non-printing characters                                                                                                                                          |               | ✓             |

The Tab Delimited Data Export option is set to escape using Spaces by default, and the CSV delimited export option is set to not replace non-printing characters by default. These default settings work under most circumstances and should be used if you are unsure about which settings to choose.

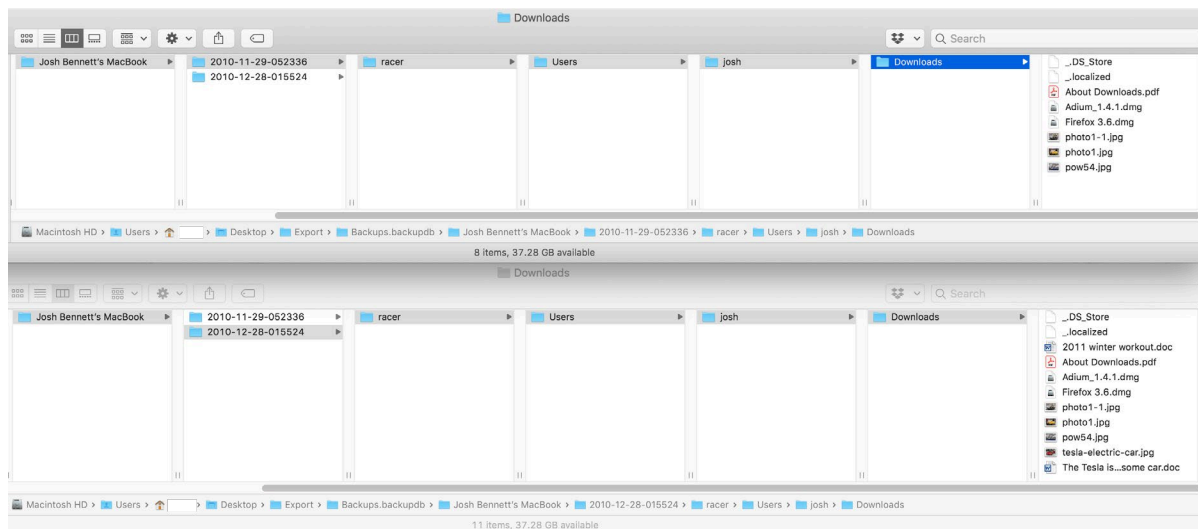
In the Exporting Files section, you can manage several options.

NTFS files may contain alternate data streams (ADS). When exporting an NTFS file, if **Export alternate data stream (ADS) with file content** is selected, the ADS will be exported with the file.

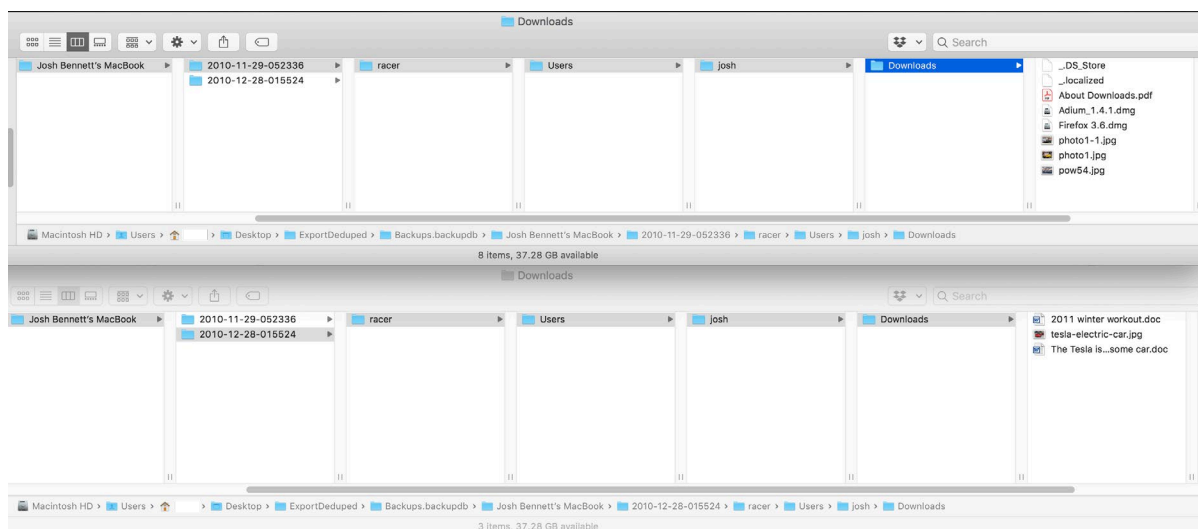
To export only unique files from a Time Machine backup, mark the checkbox for **Dedupe Hard Links**.

Time Machine backups, including the backups stored on a Time Capsule, contain incremental backups of a macOS system. These backups are stored in the folder *Backups.backupdb*, which stores date/time folders for each backup. On Time Capsule, the *Backups.backupdb* folder is stored in a sparsebundle. Time Machine backups are incremental but use Hard Links to give the appearance of full backups in each date/time folder. Once the first backup is created, Time Machine creates Hard Links in subsequent date/time folders that serve as pointers to the original files. When the next backup is made, only the files that have changed are copied into the backup and Hard Links are created for files that are not changed. When Inspector processes a Time Machine backup, all the files and Hard Links are processed. Consequently, there can be millions of files and Hard Links in each Time Machine backup. When a folder is Exported from a Time Machine backup, the Hard Links are resolved, exporting the same file multiple times.

This is an Export from a Time Machine backup showing a Downloads folder. Notice the files from the first snapshot (2010-11-29-052336) are also exported in the second snapshot (2010-12-28-011524).



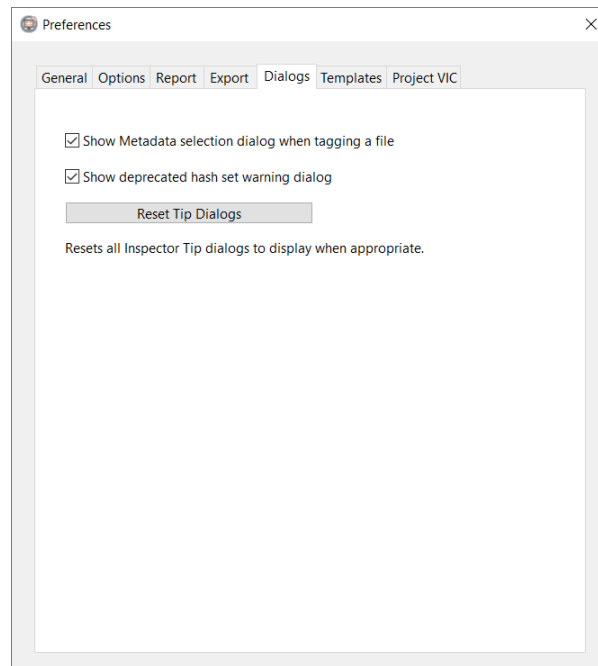
When the same folder is exported with the Dedupe Hard Links option selected, the files that were Hard Links in the second Time Machine snapshot are not exported; only the new files are exported.



The L01 Segment Size (MB) field specifies the segment size for Logical Evidence Files. By default, the size is set to 0; this means that any data exported to Logical Evidence Files is not segmented. The other options are 100, 250, 500, 1000, 5000 and 10000 (MB).

## Dialogs Tab

On the Preferences window, click **Dialogs**.



During the course of using Inspector, you can choose to hide dialogs. To show these dialogs again, click **Reset Tip Dialogs**.

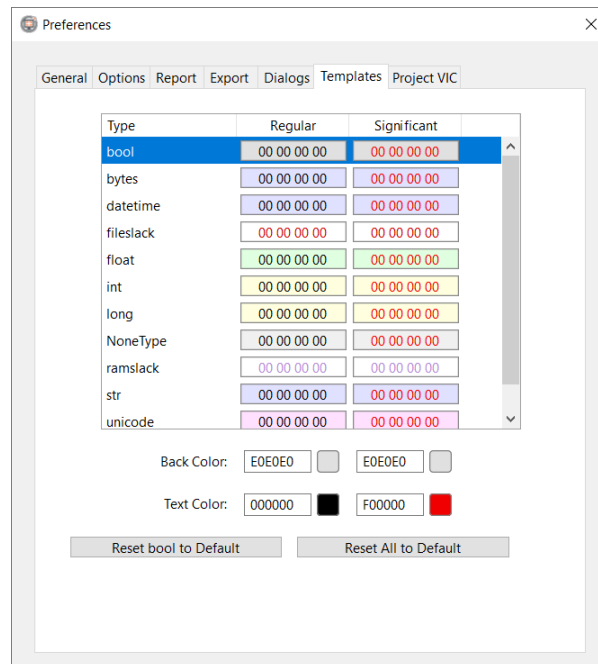
During the course of using Inspector, you can unmark the **Always show this dialog when tagging files** checkbox. However, if a user did this, you can override it by marking the checkbox for **Show Metadata selection dialog when tagging a file**. This ensures Metadata selection dialog always appears.

To force the deprecated hash set warning dialog to always appear, mark the checkbox for **Show deprecated hash set warning dialog**.



## Templates Tab

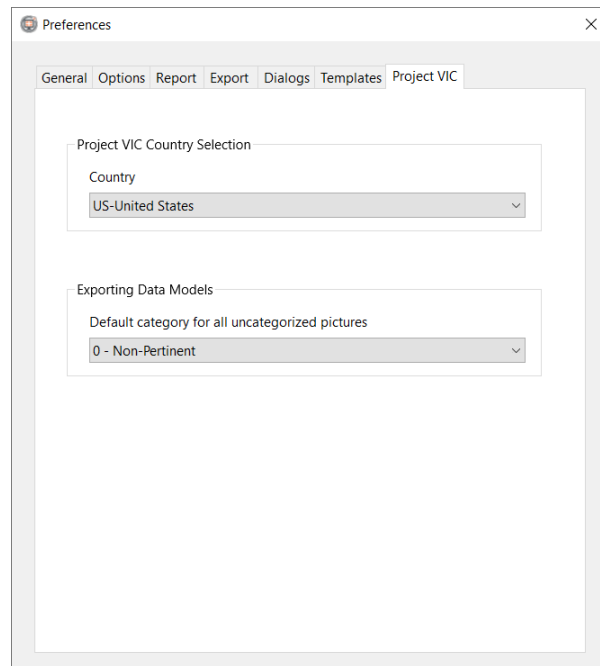
On the Preferences window, click **Templates**.



This lets you modify the color coding for data types shown in hex templates. For more information, see [Hex Templates and Data Structure View](#).

## Project VIC Tab

On the Preferences window, click **Project VIC**.



This tab provides setting selections for Project VIC Version 2.0 as well as older Project VIC versions and other data models. Project VIC Version 2.0 includes country data and corresponding category descriptions. Choose the appropriate country in the **Country** field under Project VIC Country Selection. These countries are available.

- CA-Canada
- CH-Switzerland
- DK-Denmark
- EE-Estonia
- FR-France
- NO-Norway
- RO-Romania
- SE-Sweden
- UK-United Kingdom
- US-United States

You can continue support for older versions of Project VIC and other data models. Under **Exporting Data Models**, you can set a default category when exporting uncategorized images, videos, and thumbnails to a specific data model format. These are the supported formats.

- Project VIC Version 1.1
- Project VIC Version 1.2
- Project VIC Version 1.3
- Project VIC Version 2.0
- BlueBear LACE
- C4ALL
- S21

## System Preferences on Mac Computers

These preferences should be set according to the user preferences.

### Language

1. Click **Apple > System Preferences**.
2. Click **Language & Region** (on older OSX computers, this is **Language & Text**).
3. Select the appropriate default language and drag it to the top of the list.

### Region

Different geographic locations treat date, time and numeric formats differently. In some parts of the world, dates are written with the day first, then the month and the year. In other parts of the world, the month is written first, then the day and the year.

- In Language & Region preferences, select the appropriate location in the **Region** field. Inspector displays the new date, time and numeric format settings according to the new setting.

### Date and Time

1. At the top of the Preferences window, click **Show All** to return to the main System Preferences window
2. Click **Date & Time**.
3. Choose one of these actions.
  - To manually set the current time zone and date, click the **Date & Time** tab.
  - To use the automatic clock sync feature, click the **Time Zone** tab.



## Time Format

The Clock preference is the most important setting because it determines how Inspector displays timestamps.

1. Click the **Clock** tab to set the time format.
2. Choose one of these options.
  - 24-hour format
  - 12-hour format with AM and PM displayed

## System Settings on Windows 10 Computers

One strategy concerning Time Zone configuration involves setting the Forensic System to UTC, no adjustment for daylight savings. Since Inspector will assume the same time zone as the Forensic System, this configuration may make sense. This strategy is of particular benefit if there are time zone discrepancies or if the evidentiary system traveled between time zones. The benefit comes in having a baseline date/time to work with; one that does not adjust based on location or date. Once a particular timeframe of relevance is determined, all time conversions can be calculated from that standard UTC baseline.

### Set Time Zone and Disable Daylight Savings Time

1. In the Windows search box, type **time zone**.
2. Click **Change the time zone**.  
The Date & time page of the Settings window appears.
3. In the **Time zone** field, choose the appropriate time zone.
4. Toggle Off the setting to **Adjust for daylight saving time automatically**.
5. Below Related Settings, click **Date, time, & regional formatting**.
6. On the Region page, choose the appropriate country or region.

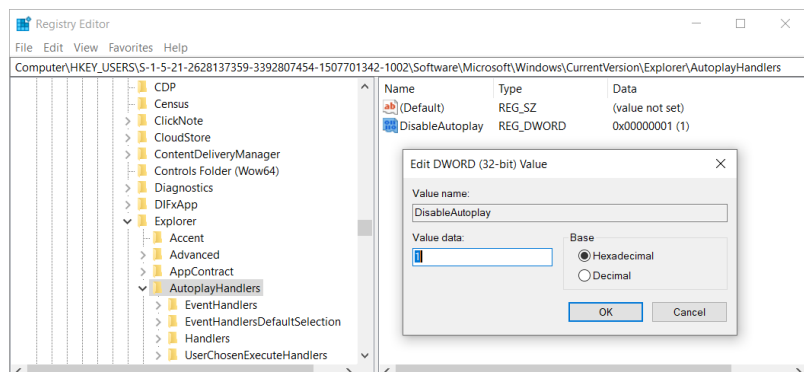
### Disabling Windows AutoPlay

The Windows AutoPlay function allows a computer to automatically start applications on removable and attachable media. Once a device (CD, iOS device, Android device, etc.) is attached, a category populates under Devices. The user can select a default action for each individual device and category. The best practice is to minimize the chance of automatic processes launching.

1. In the Windows search box, type **AutoPlay**.
2. Click **AutoPlay settings**.  
The AutoPlay page of the Settings window appears.
3. Toggle off the setting to **Use AutoPlay for all media and devices**.
4. Below Choose AutoPlay defaults, set both **Removable drive** and **Memory card** to **Take no action** or **Ask me every time**.

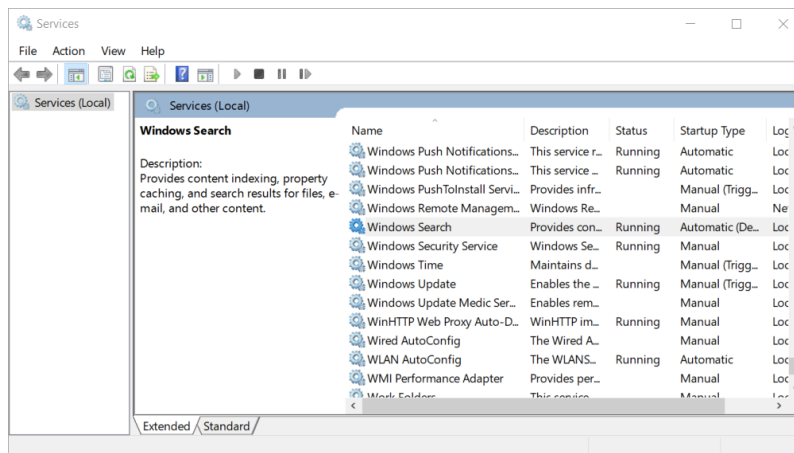
Disabling AutoPlay creates a Registry key for the logged-in user at *HKEY\_USERS\<SID of Relevant User Account>\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers*.

The created key is named **DisableAutoplay** with a DWORD (32-bit) value of 1. Therefore, you can manually configure the setting in the Registry editor.

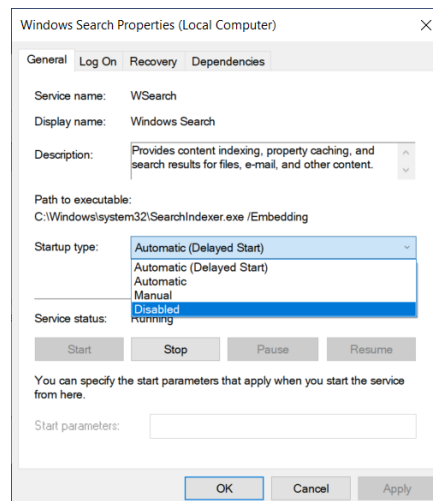


## Disable Search Indexing

1. In the Windows Search box, type **Services**.
2. For **Services**, click **Run as administrator**.  
The Services window appears.



3. Right-click the **Startup Type** value, click **Properties**, and then click **Stop**.
4. In the **Startup type** field, click **Disabled**.



5. Click **Apply**.

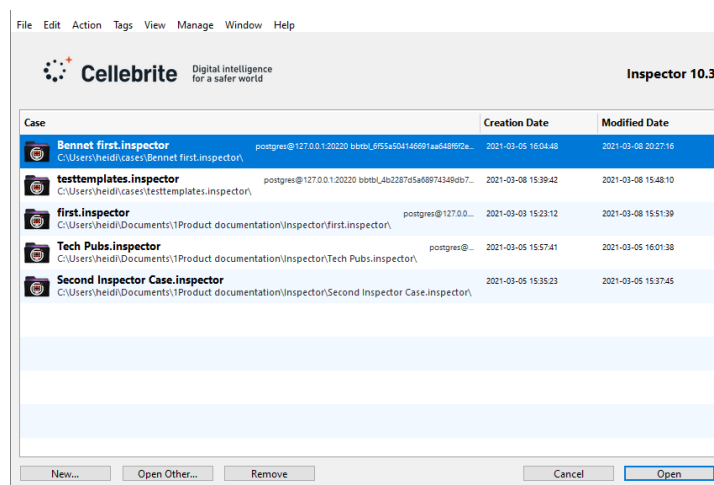
## Managing Case Evidence

This chapter provides these topics about managing case evidence.

- [Create a New Case](#)
- [Open a Case](#)
- [Adding Evidence to a Case](#)
- [Remove Evidence from a Case](#)
- [Move a Case File to a Different Computer](#)
- [Relocating a Disk Image](#)
- [Exporting Mobile Device Evidence](#)
- [Hashing and Verifying Forensic Evidence](#)
- [Advanced Evidence Recovery](#)
- [File Entropy](#)

## Create a New Case

Launch Inspector, or if Inspector is already running, click **Window > Cases Window**. The Inspector Case Manager window appears.



To create a new case, click **New**. In the Save dialog box, navigate to the location where case files are saved, and then click **Save** to save the new case and begin working with Inspector.

On Windows computers, an Inspector case can be mapped to a volume letter of your choice, thus avoiding the file path character limit of Windows. Inspector defaults to the next available drive letter, but you can choose the drive you prefer by clicking **Manage > Drive Mappings**. After you map the case to a drive letter, close the case and then open the Case Manager window. Click **Open Other** and locate the case you just mapped.

When you open a case file, the Case Info view appears. You can provide information about the examiner and the case here. You can change or add to this information any time during an examination.

The Examiner Information fields retain the information you provide; you don't need to provide this information each time you create a case.

Because each case is unique, you must provide the case number, case name, and synopsis for each case in the Case Information fields.

Inspector detects if it has not been updated recently and notifies you when an update is available, with links that provide access to necessary updates.

## Inspector Time Zone Settings

In the bottom left corner of the Case Info window, you may select a time zone in the Time Zone field. This determines the time zone used by evidence timestamps in the Case Window and in the examiner report.

By default, Inspector displays timestamps as Coordinated Universal Time (UTC). Dates and times are displayed with the selected time zone appearing in parentheses, for example: 2009-12-19 19:34:51 (PST). Inspector makes automatic adjustments for daylight savings time shifts for different parts of the world. You don't need to make any manual changes.

After case information is complete, you can begin adding evidence to the case file.

On a Mac computer, an Inspector case file is actually a package file.

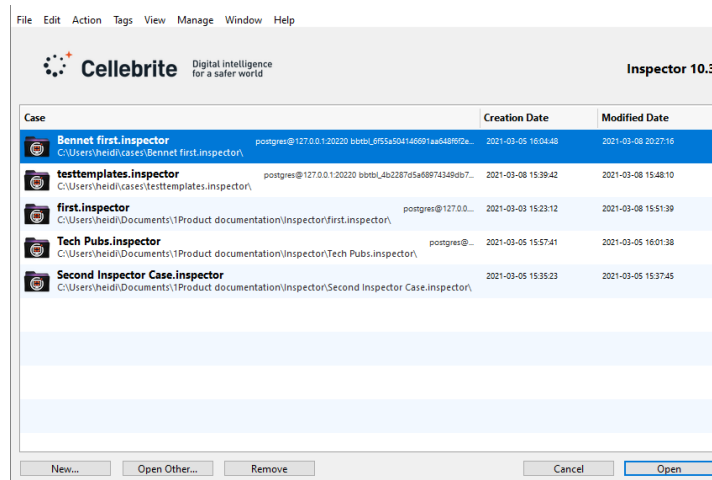
On a Windows computer, an Inspector case is a folder.

All case elements are stored in this folder or package file, so a case file can grow rather large depending on how big a case is. Before you create a new case, make sure there is plenty of storage space on the working hard drive.



## Open a Case

Launch Inspector, or if Inspector is already running, click **Window > Cases Window**. The Inspector Case Manager window appears.



The Inspector Case Manager window shows a list of recently opened cases. To open a case file, select the case and click **Open**. To reopen a case after it has been removed from the recent case list, click **Open Other**, navigate to the case file, and then click **Open**. You can open a case located anywhere in the file system.

- On Windows computers, double-click the case file in File Manager.
- On Mac computers, double-click the case file in Finder. You can also drag a case file from Finder onto the Inspector Case Manager window to add it to the recent case list.

If the case list becomes too long, you can remove items from the list. Open the context menu from a case, and then click **Delete from recent item list**. You can also select a case and press DELETE. This removes the case from the list but does not delete the case file itself. To see the location of a case file in the file system, open the context menu from the case, and then click **Reveal on Disk**.

## Update a Case to Work in a Newer Version of Inspector

If you open a case that was created using a version of Inspector that is older than the version currently running on your computer, this message appears: **The case document is out of date. Would you like to update the document now?** Click **Update** to update the case file. You can click **Cancel** to continue working with the case file without updating it, but this is not recommended.

Case files created in older versions of Inspector sometimes cannot be updated to the newest version.

Updating a case file does not automatically run any processing or analysis. To take advantage of new or enhanced processing or features, you must re-examine case data.

1. Archive the case file in the older version of Inspector.
2. Import the archived case into the newer version of Inspector.
3. Reprocess the evidence in the newer version of Inspector.

This ensures that all functions and features of the newer version of Inspector are used to analyze the data.

## Adding Evidence to a Case

These types of evidence can be ingested into a case in Inspector.

| Evidence Types                          | Description                                                                                                                                                                                                              |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disk Image                              | A forensic image. Inspector supports dd, dmg, sparse images/bundles, vmdk, E01, Ex01, L01, AFF4, and SMART image formats. Use this option to add iOS images created by: JZ, iXAM, Cellebrite, MPE+, and ElcomSoft.       |
| Selected Image File                     | A selected image file or virtual machine file is an evidence item in the Component list (available only when an image file or VM file is selected)                                                                       |
| Unencrypted or Encrypted iOS Disk Image | An unencrypted iOS disk image, or a forensically-acquired third-party iOS disk image with proprietary encryption enabled (for example, Cellebrite, Lantern Lite, etc.)                                                   |
| iOS Backup                              | An iOS device (such as iPhone or iPad) backup folder                                                                                                                                                                     |
| Memory (Dump, Image, File)              | A Windows memory (RAM) file. Inspector supports raw, <i>hiberfil.sys</i> (Hibernation file, from Windows Vista through Windows 10 v1703), <i>pagefile.sys</i> , and crash dumps (full, from Windows Vista or Windows 7). |
| USB Attached Mobile Device              | A mounted iOS device (iPod, iPhone or iPad), or Android device                                                                                                                                                           |
| Other Attached Device                   | A mounted device such as a .dmg image, a Time Machine, an external FireWire or USB drive, or a mounted .E01 file (EWMounter)                                                                                             |
| Mobilyze Case                           | A case from Mobilyze, Cellebrite's mobile device triage tool                                                                                                                                                             |
| Folder                                  | A folder and the folder's contents                                                                                                                                                                                       |
| File                                    | An individual non-disk image file                                                                                                                                                                                        |
| Berla Inspector .ivx Database           | A database exported from Berla iVe Desktop using the Cellebrite export option                                                                                                                                            |
| iCloud Production Files from Apple      | iCloud zip archives extracted from encrypted GPG files containing iCloud device backups within. These files can be obtained from Apple with a valid search warrant.                                                      |

You can add disk image files, folders, iOS backups, and other external files by dragging and dropping them from the source (Finder, external device, etc.) onto the Evidence section of the Component list. Inspector imports these image formats.

| Disk Image Formats                                                       | Creation Program                                                               |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| RAW Image (DD)                                                           | Most Forensic Programs                                                         |
| Disk Image (DMG)                                                         | Digital Collector, Converted DD images                                         |
| EnCase (EWF-E01), (EWF-L01), (EWF2-EX01)                                 | EnCase (all versions), FTK Imager                                              |
| SMART (EWF-S01)                                                          | ASR Smart                                                                      |
| Virtual Machine Disks (VMDK) including for Windows 10                    | VMware                                                                         |
| Advanced Forensic File Format (AFF4)                                     | Digital Collector                                                              |
| iOS Image Formats                                                        | Vendor                                                                         |
| Cellebrite UFED PA (1.1.7.8 and higher) Physical Images                  | Cellebrite                                                                     |
| Premium CAIS extractions (.dar format)                                   | Cellebrite                                                                     |
| Cellebrite Logical Images created via Method 1 (iOS backup archive)      | Cellebrite                                                                     |
| Cellebrite Logical Images created via Method 2 (logical filesystem dump) | Cellebrite                                                                     |
| GrayKey                                                                  | Grayshift                                                                      |
| iOS Forensic Toolkit (1.04 and higher)                                   | ElcomSoft                                                                      |
| iPhone-Dataprotect / Lantern Lite                                        | <a href="http://code.google.com">http://code.google.com</a> / Katana Forensics |
| JZ (all versions)                                                        | Jonathan Zdziarski Tools                                                       |
| iXAM (2.3.9 and higher)                                                  | Forensic Telecommunications Services                                           |
| MPE+ (4.0 and higher) Physical Images                                    | AccessData                                                                     |

Inspector allows multi-core processing during device acquisition to speed up parsing, paths, file types, picture, video, and metadata processing. You can change this setting on the Options tab in the Preferences window. For more information, see [Inspector Preferences or Options](#).

**Note:** A physical drive acquisition produces a bit-by-bit forensic image and allows a forensic examiner to view the full contents of a drive or device, including contents that an operating system might not “see.” A logical acquisition is a collection of items, such as files and folders, that an operating system likely would “see” under normal circumstances.

Both types of acquisitions must be authenticated or “hashed” to confirm the copy is identical to the original.

A forensic image (.dmg) is identical to the disk or device from which it was acquired and includes allocated, unallocated, and free space. It is a bit-by-bit representation of the entire physical drive or device. A .dmg disk image acts like a hard drive, but it is actually a single file. It can be resized using an application such as Apple’s Disk Utility application.

A sparse image (.sparseimage) is also a single file, but it becomes larger as additional data is added to it. A sparse image is a logical representation of the logical data copied to it.

A sparse bundle is a bundle (like a folder) that contains several individual files. A sparse bundle is also a logical representation of the logical data that has been copied to it.

## Supported File Systems

Inspector’s filesystem parsers include parsers for the Apple File System (APFS), HFS+/HFSX filesystem, FAT filesystems (FAT12/FAT16/FAT32), and NTFS filesystem. Inspector will allow ingestion and parsing of other filesystems however, support is currently experimental as they have not been fully tested within Inspector.

Experimental filesystem parsers: exFAT, EXT2, EXT3, EXT4, UFS, YAFFS2, ISO 9660.

## Add Evidence Items

You can add evidence files to a case in Inspector from the Component list by dragging and dropping, or from the File menu.

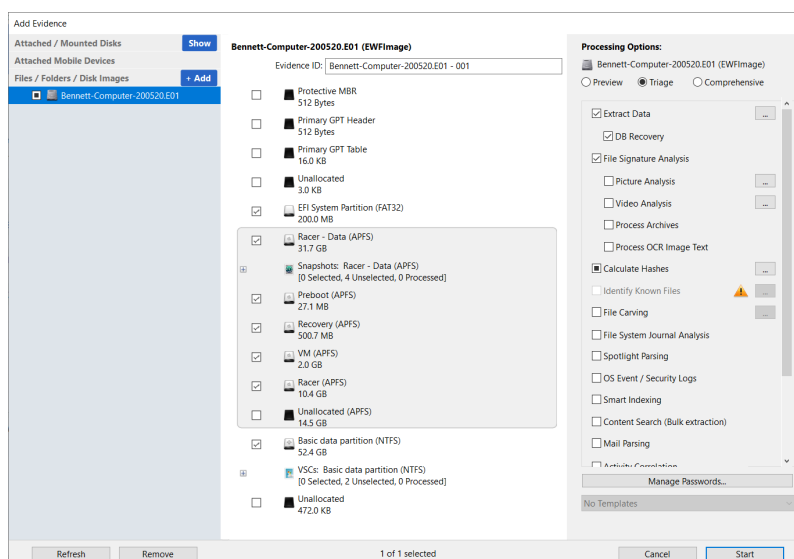
- Click **File > Add Evidence**.
- In the Evidence section of the Component list, click **Add**.

The Add Evidence window appears with all appropriate options for data ingestion. Inspector automatically scans for attached or mounted live devices, including attached and unlocked mobile devices, for display in the upper left under Attached/Mounted Devices. Attached disks or volumes are hidden by default, but you can see or hide them by clicking **Show** or **Hide**. Below that are any files, folders, memory images, and disk images that are potentially being added to the case. (Each item has a checkbox that can be selected or deselected. The item will only be included in the ingestion process if the item’s checkbox is activated.) To remove an item from this list, open Inspector’s context menu from the item and click **Remove**. To add an item to the list, click **Add**, then choose the appropriate disk image, folder, or file.

**Note:** When you click **Add** on a Windows computer, a dialog box appears prompting you to choose either **Add File** or **Add Folder**. To add a forensic disk image, memory image, mobile device image, or a file, click **Add File**. (If you are adding a disk image that is segmented, only the first segment needs to be selected.) To add an iOS backup, a Mobilyze case, or other folder structures, select **Add Folder**.

It is possible to add multiple items to a case at the same time. Select each item for processing and choose the desired ingestion options.

Click **Refresh** at the bottom of the window, and Inspector once again scans for attached or mounted live devices, including attached and unlocked mobile devices, and displays them in the upper left.



When an item is selected in the left pane, all its partitions are displayed in the middle pane. Partitions with recognized file systems display with activated checkboxes by default, while partitions with non-recognized file systems do not have activated checkboxes. APFS Snapshots and Windows Volume Shadow Copies (VSCs) are also displayed in the middle pane with an expansion arrow. Underneath each Snapshot and VSC entry is a label indicating the number of Snapshots or VSCs Selected, Unselected and Processed. By default, none of the Snapshots and VSCs are selected for processing. Like all other volumes listed, different processing options can be set for each individual Snap and VSC. Keep in mind, processing all Snapshots and VSCs will take time. They do not have to be ingested during initial evidence processing.

If you mark the checkbox for a partition with a non-recognized file system, **Carve Unallocated** then becomes an available option for that partition.

Any partition with a recognized file system may also be imported as unallocated. Open Inspector's context menu from the partition and click **Import Partition as Unallocated**. The **Carve Unallocated** option becomes available for that partition.

Attached disks in the left pane can also be imported as unallocated in the same fashion. Open Inspector's context menu from the item and click **Import as Unallocated**.

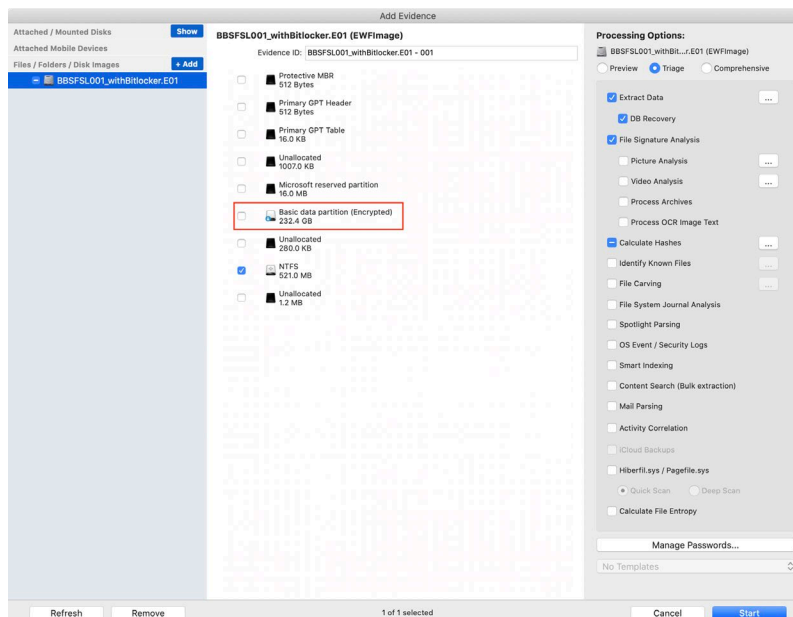
**Note:** If the item is a partition with a recognized file system that is currently set for adding to the case as unallocated, Import Partition Normally is an available option in the context menu.

If you click **Add** and select a memory file to add to a case, Inspector usually recognizes it as a memory file. However, some memory files are so complex that Inspector cannot instantly determine whether they are memory images. If Inspector is unable to verify a memory file within 10 seconds, the item is displayed as a plain file. You may override this interpretation and tell Inspector to ingest the item as a memory file. Open Inspector's context menu from the item and click **Memory (Dump, Image, File)**.

Passware is integrated into Inspector. Images with these types of full disk encryption can be decrypted with the proper decryption credentials.

- BitLocker
- FileVault 2
- LUKS (Linux Unified Key Setup)
- TrueCrypt
- VeraCrypt

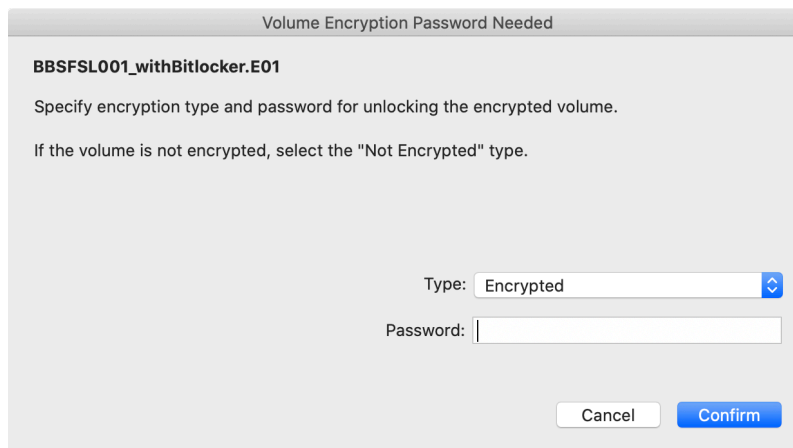
When an image file using one of these encryption types is added to Inspector, it is identified as a locked partition.



When the locked volume is selected, the Volume Encryption Password Needed dialog box appears.

- BitLocker requires either the password or recovery key for decryption.
- FileVault 2 requires a user login password.
- LUKS requires the password or recovery key.
- TrueCrypt and VeraCrypt volumes, select the encryption type, and then type the password. A VeraCrypt volume may also require the optional PIM (personal iterations multiplier). VeraCrypt may take several minutes to validate the password.

**Note:** Hidden volumes are not supported.



A screenshot of a Windows-style dialog box titled "Volume Encryption Password Needed". The dialog has a light gray background. At the top, the title bar is dark gray with the text "Volume Encryption Password Needed" in white. Below the title bar, the text "BBSFSL001\_withBitlocker.E01" is displayed. Underneath, there are two lines of instructional text: "Specify encryption type and password for unlocking the encrypted volume." and "If the volume is not encrypted, select the 'Not Encrypted' type." In the center, there is a "Type:" label followed by a dropdown menu showing "Encrypted" with a blue arrow icon to its right. Below the dropdown is a "Password:" label followed by a text input field. At the bottom right, there are two buttons: "Cancel" and "Confirm".

Once the volume is unlocked, choose the processing options. The decrypted data will be displayed in Inspector.

With an item in the left pane selected, the middle pane shows an Evidence ID field where you can edit the evidence ID for the item.

**Note:** Evidence IDs can only be used to label items in the left pane. They cannot be used to label items in the middle pane, such as device partitions.

You can also perform these tasks from the Add Evidence window.

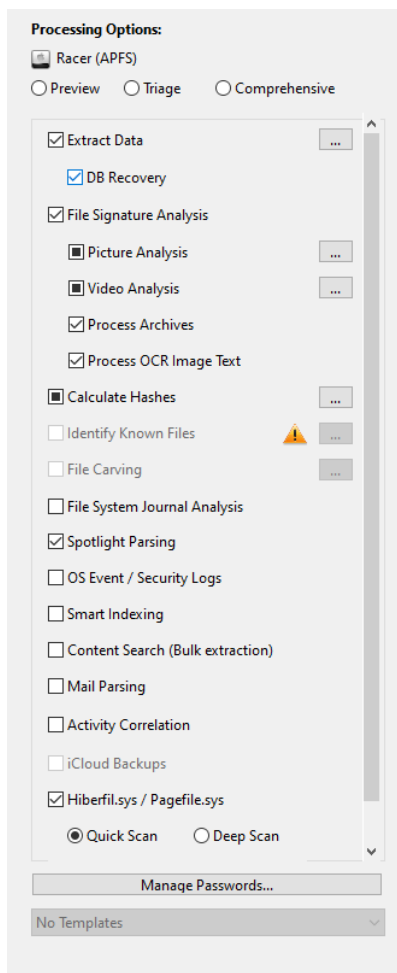
- Recover a deleted or missing partition.
- Specify disk sector size for a disk or partition.
- Create an .iso disk image file from a partition.

For more information, see [Advanced Evidence Recovery](#).

The Add Evidence window has these quick processing options for ingestion.

- Preview deselects all options.
- Triage lets Inspector automatically select only some of the options. These depend on the type of items selected.
- Comprehensive selects all options.

You can also manually select processing options for ingestion for each item or volume, Snapshot, or VSC remain so that each piece of evidence is processed in only the manner you choose.



If an item is selected in the left pane while you change ingestion options in the right pane, those options apply to all partitions in the middle pane. However, selecting a partition in the middle pane allows you to change ingestion options for just that partition, if desired.

A black square in checkbox reflects an indeterminate value, meaning that some, but not all, of the sub-options for that selection are activated. For example, if you mark the Calculate Hashes checkbox, you see a checkmark. However, when the corresponding ellipsis button is selected and only the MD5 sub-option is chosen, the Calculate Hashes checkbox shows a black square, for an indeterminate value. The same concept applies to the left pane of the Add Evidence window. If only some partitions for an evidence item are selected for import, the left content pane will show an indeterminate value for the item rather than a checkmark.

You can select custom processing options for a specific attached device and have them remembered. This lets you close the case and open it later in the Add Evidence window without having to select processing options again. You can change this setting on the Options tab in the Preferences window. For more information, see [Inspector Preferences or Options](#).

You may also use saved ingestion option templates. Choose the appropriate template in the Saved Templates field in the lower right of the Add Evidence window, and the ingestion options immediately update to reflect the saved template settings. For more information, see [File Menu](#).



## Adding a Disk Image

The process for adding a disk image is begun the same way as for adding any form of evidence to an Inspector case. For more information, see [Adding Evidence to a Case](#). Additional information about ingestion/processing options appears below.

In the Ingestion Options section of the Add Evidence window, mark the checkbox for the appropriate options.

| Option                       | Description                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Extract Data                 | Inspector's internal processes for populating data in the Actionable Intel, Communication, Locations, Internet, Productivity, and System tabs.                                                                                                                                                                                                                                   |
| DB Recovery                  | Recovers deleted entries from databases                                                                                                                                                                                                                                                                                                                                          |
| File Signature Analysis      | Compare file headers to file extensions to see if they match (populates Content Extension field)                                                                                                                                                                                                                                                                                 |
| Picture Analysis             | Identify pictures using signature analysis, options include running Image Analyzer against pictures identified for selected threat categories                                                                                                                                                                                                                                    |
| Video Analysis               | Parse videos and split them into sixteen frame sequences (4 x 4) to allow Inspector gallery view and % skin tone analysis, options include running Image Analyzer against the sixteen frame sequences created for each video identified for selected threat categories                                                                                                           |
| Process Archives             | All archive files (zip, gz, 7z, tar, and rar) are expanded down to two levels of nested archives                                                                                                                                                                                                                                                                                 |
| Process OCR Image Text       | Process image (picture) files to extract text. Optical character recognition (OCR) converts text detected in the image into plain text which can be indexed and then searched. This process can be slow and is limited to these image types. <ul style="list-style-type: none"> <li>• pdf</li> <li>• tiff</li> <li>• bmp</li> <li>• png</li> <li>• jpg</li> <li>• gif</li> </ul> |
| Calculate Hashes             | Hash all files using MD5, SHA-1 and SHA-256 algorithms                                                                                                                                                                                                                                                                                                                           |
| Identify Known Files         | Identify known file types using Known File Hash (KFH) databases                                                                                                                                                                                                                                                                                                                  |
| File Carving*                | Recover or attempt to recover deleted files based on defined File Signatures                                                                                                                                                                                                                                                                                                     |
| File System Journal Analysis | Process <i>\$USNJRL</i> and <i>\$LogFile</i> files in Windows and <i>macOS .fsevents</i> (results are displayed in the System tab in the System Logs sub-view)                                                                                                                                                                                                                   |

| Option                           | Description                                                                                                                                                                                              |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Spotlight Parsing                | macOS Spotlight extended attribute data parsing                                                                                                                                                          |
| OS Event / Security Logs         | Windows EVT/EVTX analysis, macOS ASL logs, and macOS Unified Logs (results are displayed in the System tab in the System Logs sub-view)                                                                  |
| Smart Indexing                   | Create a Smart Index of processed allocated data                                                                                                                                                         |
| Content Search (Bulk Extraction) | Runs built-in searches against memory files                                                                                                                                                              |
| Mail Parsing                     | Processes Apple Mail, Outlook mail files                                                                                                                                                                 |
| Activity Correlation             | Identifies correlated events done by the system, by a user, or by device.                                                                                                                                |
| iCloud Backups**                 | Processes iOS device backups from decrypted iCloud Production files (obtained via search warrants from Apple)                                                                                            |
| Hiberfil.sys / Pagefile.sys      | Processes Windows memory hibernation file and pagefile. If <i>hiberfil.sys</i> and <i>pagefile.sys</i> files are located, Inspector processes them as separate Evidence items within the Component list. |
| Calculate File Entropy           | Determines possible encryption level of files                                                                                                                                                            |
| Manage Passwords***              | Enter a password, list of passwords, or import a file containing passwords (UTF-8 encoded, one per line), to unlock and parse Apple keychains on macOS or iOS devices                                    |

\*This option will be seen as Carve Unallocated if importing an item as unallocated.

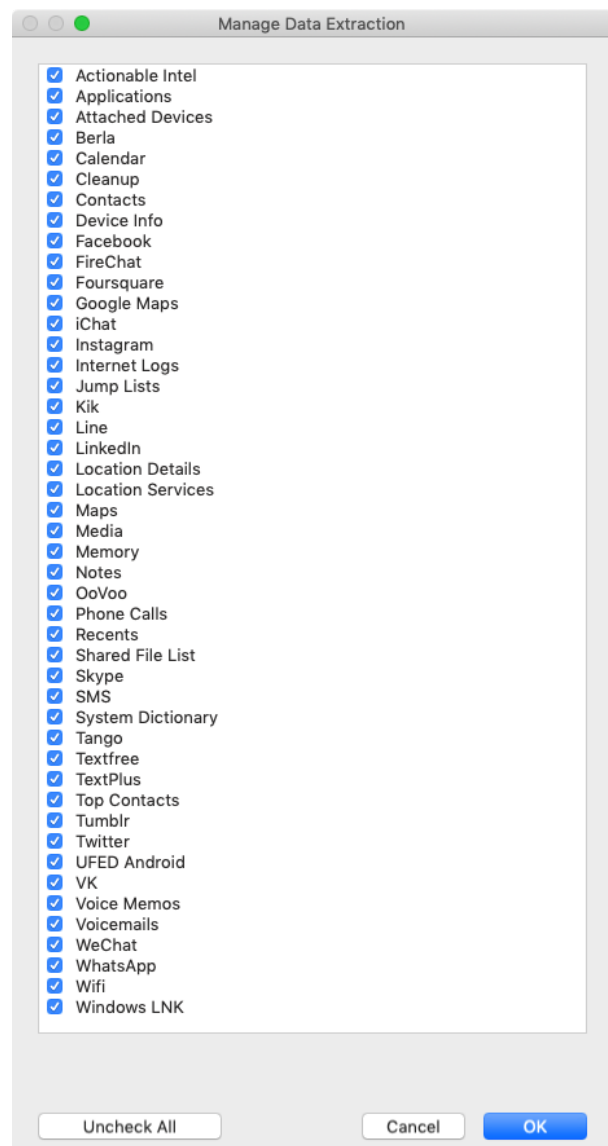
\*\* This option is only available when ingesting data from iCloud production files. For more information, see [Adding iCloud Productions](#).

\*\*\*Inspector will only attempt to unlock Apple keychains with the passwords entered during initial evidence ingestion. For more information, see [Actionable Intel View](#).

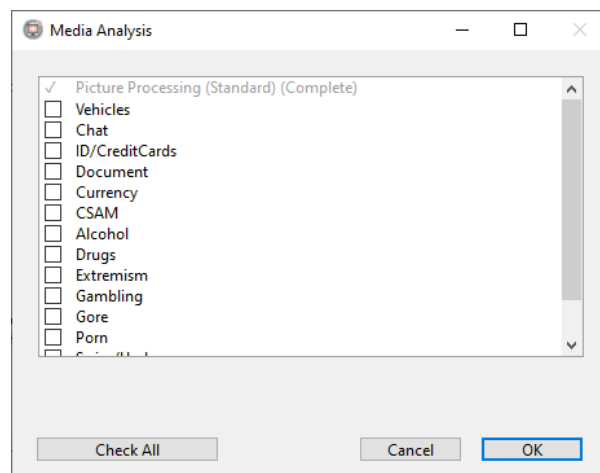
These ingestion options have corresponding ellipsis buttons providing additional options.

- **Extract Data:** the Manage Data Extraction window lists all items that are normalized
- **Picture Analysis:** the Media Analysis window provides options for standard picture processing and image classification categories provided by Image Analyzer
- **Video Analysis:** the Media Analysis window provides options for standard video processing and image classification categories provided by Image Analyzer
- **Calculate Hash:** the Hash Types window lists the three hash algorithms available in Inspector for file hashing (MD5, SHA1, and SHA256)
- **Identify Known Files:** the Hash Sets window allows the examiner to choose which hash sets Inspector should use to identify known and notable file types
- **File Carving:** the File Signature Management window shows the defined file signatures used for file carving

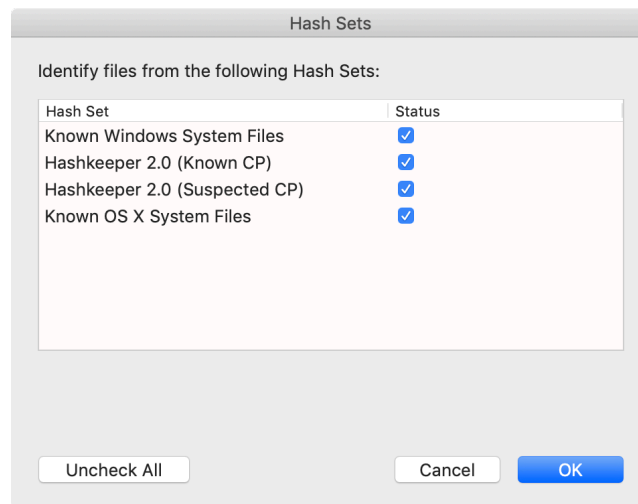
Extract Data refers to the internal Inspector processes used to generate the data displayed in the Actionable Intel, Communication, Locations, Internet, Productivity, and System tabs, with the exception of Windows registry files in the System tab. Registry files are parsed with filesystem parsing. Examiners can choose to limit which data extraction processes are run by deselecting options in the Manage Data Extraction window, focusing on the data pertinent to the examination. In the bottom left corner of the Manage Data Extraction window, click **Uncheck All**. Then select only the desired processes and click **OK**.



Standard Picture and Video processing populates the Media tab. The Image Analyzer classification categories include: Alcohol, Chat, Child Sexual Abuse Material (CSAM), Currency, ID/CreditCards, Document, Drugs, Extremism, Gambling, Gore, Porn, Swim/Underwear, Vehicles, and Weapons. Examiners can choose to run any or all of these categories against pictures and videos. Classification of videos is determined using the Inspector-generated 16 image (4 x 4) mosaic containing still frames from the video. By default, Inspector runs only standard picture and video processing. For additional image categorization, click on the ellipse button. On the lower left side of the Media Analysis window, click **Check All** to classify with all available classification categories. Otherwise, select only the desired categories. Click **OK** once the desired options are selected.

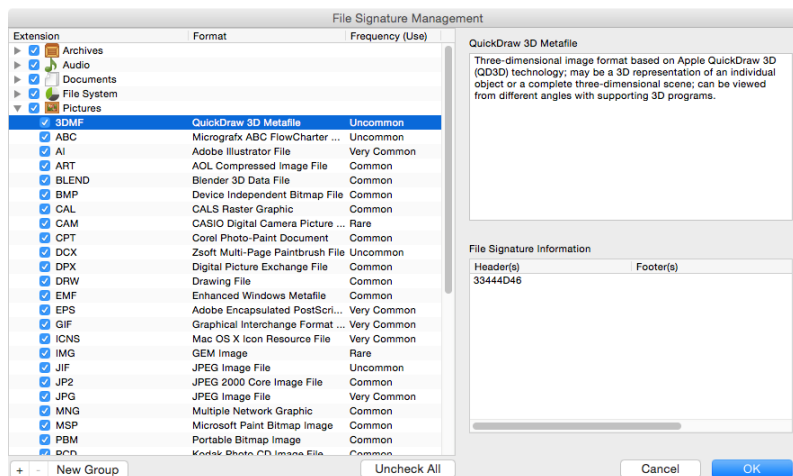


To help identify known files, Inspector ships with the Known OS X System Files, Known Windows System Files, and the Hashkeeper hash sets. Additionally, Inspector recognizes Encase (6.19 and lower), NSRL (full), and Inspector (.blhs) hash set formats. Inspector also imports hash sets saved as text files as long as the file contains one hash value per line with each line separated by a carriage return. Hash sets can be created from files in a case using any or all of the available hash types (MD5, SHA-1, SHA-256). Custom hash sets created in Inspector are automatically saved in the .blhs format and are available for use in all Inspector cases. The Calculate Hashes ingestion option must be selected for Identify Known Files to work. By default, hash comparisons are performed using MD5 hash values. You can change this default. For more information, see [Inspector Preferences or Options](#).



When File Carving, by default Inspector attempts to recover all listed file types. This may take some time. In the ingestion options, if activating the File Carving checkbox (or Carve Unallocated if importing an item as unallocated), select the corresponding ellipsis button for further options. A separate File Signature Management window opens. Here the examiner may specify the unallocated file types to include in the recovery attempt. For more information, see [Advanced Evidence Recovery](#).

Below the Frequency column in the File Signature Management window, click **Uncheck All**. To the left of a file type group, select the disclosure triangle to reveal individual file types within the group and select only file types of interest to shorten the processing time. For more information about a given file type, select the file type to highlight it, and the right half of the File Signature Management window displays a verbal file type description and a list of typical file headers and footers (if available) for the selected file type.



An examiner may also create custom, user-defined file signature databases. Once created, these user-defined databases appear in the File Signature Management window, and an examiner may add additional file signatures to the database or remove existing signatures from the database directly from this window. By default, user-defined file signature databases are stored in the */Application Support/Cellebrite/Inspector/UASignatureDBs* folder. For more information, see [File Signature Databases](#).

Inspector offers the capability of calculating byte stream entropy per file, which can aid in discerning between items that are more likely to be encrypted versus those which are not. Entropy values range from 0 to 1, with values closer to 1 denoting items that are more likely to be encrypted. To use this feature, select **Calculate file entropy**. After processing for file entropy on an evidence item, values are displayed under the Entropy column in the Browser and File Filter views. Entropy is available as a sortable column for display in the Browser and File Filter views.

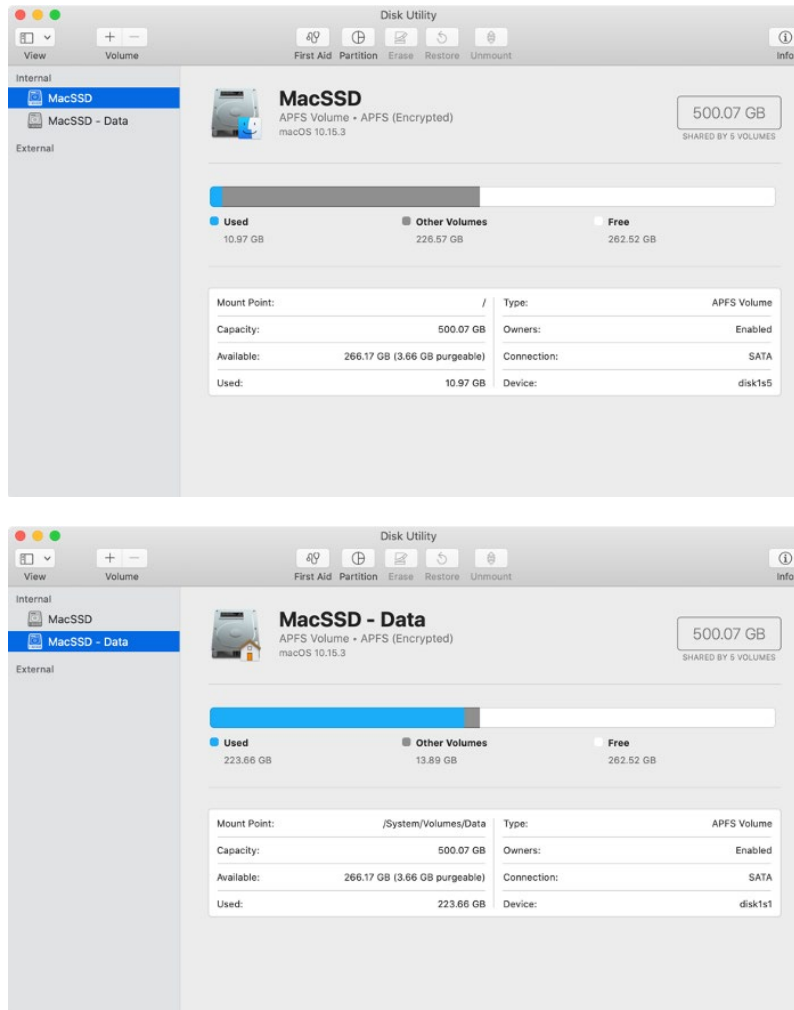
A bulk extraction tool is used to perform content searches on memory files, scanning the evidence file for key items of interest. For more information, see [Bulk Extraction Searches on Memory Files](#).

**Note:** Only processing options that apply to the selected evidence item are shown as available. Options not selected at the time an evidence item is being added to the case can be run later from the Evidence Status view by selecting the **Run** button for the process.

## APFS on macOS 10.15

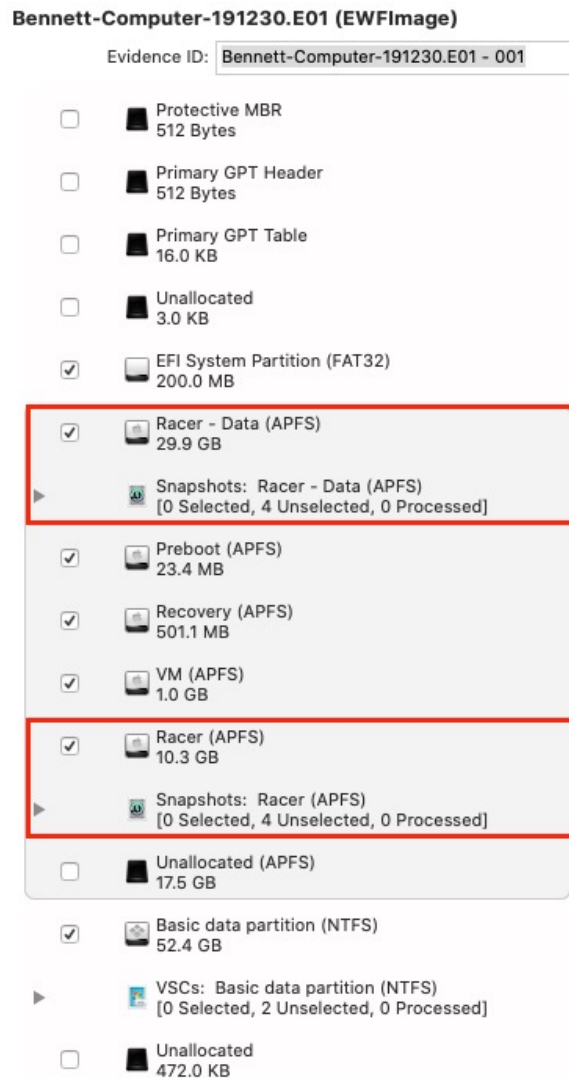
With the release of macOS 10.15, increased system protection was added to macOS. macOS Catalina runs in a read-only system volume, separate from other files. When a system is upgraded to Catalina, a second volume is created, and some files may move to a Relocated Items folder.

The boot volume was split into two pieces. On the Desktop it appears as one volume, but looking at it via Disk Utility, it is readily apparent there are two volumes:



The volume name that appears on the Desktop appears in both volumes; the second volume has - Data appended to the volume name. For more information, see this topic provided by Apple: <https://support.apple.com/en-us/HT210650>.

This structure can also be seen when the volume is processed in Inspector. This can first be seen when ingesting evidence with a macOS 10.15.



This example shows a macOS system with the volume name Racer. Evidence processing options can be different for the two volumes and the associated APFS Snapshots. User files and data are stored on the <Volume Name> - Data volume. The system data is stored on the <Volume Name> volume and is mounted read-only when macOS is running. In addition, the system volume contains system .plist and database files, and system applications (pre-installed Apple applications). When choosing processing options keep this in mind.



## Starting the Evidence Ingestion

When finished with the options in the Add Evidence window, select the **Start** button to start the data ingestion. In the Component list select Evidence Status. Inspector begins ingesting and processing the data according to the options chosen.

As soon as the file system is parsed, a check box will appear in the Component list for that evidence item. The examiner can then browse the evidence item in the Browser tab while the other processing options are finishing.

## Running or Rerunning Processing Options After Ingestion

To run previously skipped file processing options at any time, in the Component list under Activity, select Evidence Status. A Run button appears for the processing options that have yet to execute. Click **Run** to execute the associated file processing option. Evidence processing status indicators appear in the Content pane. Status indicator labels display Preparing, Percentage Completed, and Finished as progress is made.

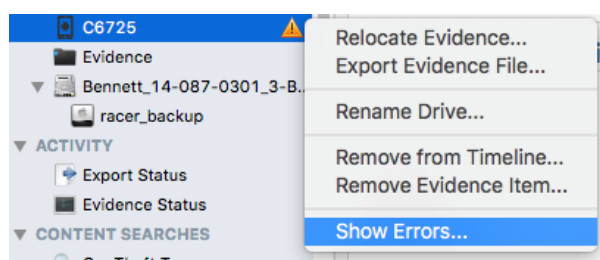
An examiner can also run the hash set processor (Known Files) and the unallocated file recovery processor (File Carving) multiple times during a case. In the Component list under Activity, select **Evidence Status**. A Run button appears in the Content pane next to Known Files. When you click **Run**, the Hash Sets window appears. Select the desired hash sets to apply during processing and click **OK**.

In the Content pane, a Rerun button appears next to File Carving for each volume or device, with the exception of APFS volumes. When you click **Rerun**, a warning dialog appears to alert the examiner that Inspector is temporarily removing the partition from the case and reprocessing the data. To proceed, click **Reset** in the warning dialog. For more information, see [File System Information](#).

**Important:** When you click **Reset**, tags associated with data contained on the partition are permanently removed from the case.

## Show Errors

If an error occurs during the acquisition, an error badge (i.e., exclamation mark within a triangle) appears in the Evidence list next to the device's name associated with the error.



From the error badge, open the context menu, and then click **Show Errors**. A window containing a list of errors that occurred during data processing appears. Click **Save to File** to save the error list to a text file.

Most data processing errors are benign, but an examiner should note these errors to preserve case integrity. FileSystemID conflict errors may indicate duplicate file creation caused by file system corruption. Inspector automatically resolves these and other common error types. In the Errors window, click **Ignore** to ignore an error. In the confirmation dialog box, click **OK**. The error badge is removed from the Evidence section in the Component list.

An examiner may also perform an unallocated recovery on an entire disk if the acquisition or data parsing process fails entirely.

## Adding a Selected Image File on an Imported Evidence Item

To add an image file located on an evidence item that is already in a case, select a device partition in the Component list, and on the toolbar click **Details**. In the Artifacts section at the lower right of the window, double-click on the Disk Images bar graph. Inspector switches to the File Filter view and displays a list of disk images.

In the Content pane, select an image file to add to the case as a new evidence item. Click **File > Add Selected**.

The Add Evidence window appears. Choose the processing options, then click **Start**. Inspector adds the image file to the case and the image appears as an item in the Evidence section of the Component list.

## Adding an iOS Disk Image or Backup

As long as you have access to the necessary encryption credentials/files, Inspector ingests and processes unencrypted or encrypted iOS disk images as well as encrypted or unencrypted iOS backup folders.

The process for adding iOS evidence is begun the same way as adding any form of evidence to an Inspector case. For more information, see [Adding Evidence to a Case](#).

## Adding Unencrypted iOS Disk Images

Use the Add Evidence window to import unencrypted bit-by-bit forensic iOS images (allocated, unallocated, and free space) acquired from iOS devices. Note however, that devices running iOS version 4.0 or higher are encrypted at the block level, and therefore full data recovery from unallocated space is not possible. Email cannot be retrieved.

Inspector ingests the following unencrypted iOS disk image formats:

- ElcomSoft
- Celebrite
- iXAM
- MPE+ (Tarball image)
- iPhone-Dataprotection & Lantern Lite

## Adding Encrypted iOS Disk Images

Some third-party iOS image acquisition tools do not create a decrypted disk image by default. Instead, the acquired bit-by-bit forensic image file remains in an encrypted state after acquisition, and a decryption key file that decrypts the image is included with the acquisition. However, some of these third-party tools do have a decrypted image acquisition option. If you select this option, a second unencrypted image is created during the acquisition process.

Inspector imports encrypted third-party iOS forensic images. However, to conserve disk space, Inspector does not use the decryption key to create a second unencrypted image. Instead, Inspector uses the decryption key to decrypt the image on the fly as the image is imported.

Inspector imports the following encrypted iOS disk image formats:

- Cellebrite (.ufd)
- MPE+ (dd8 images that are not pin-locked)
- iPhone DataProtect & Lantern Lite

When adding an encrypted iOS forensic image to a case, the Open Decryption Key File window appears. Select the decryption key file and click **Open**.

Inspector imports the encrypted disk image and uses the decryption key to decrypt the image on the fly as the image is imported.

## Adding iOS Backup Folders

Inspector acquires logical data from an iOS backup file (i.e., iTunes backup). An iOS backup file may not contain current data, but data recently deleted from an iOS device may be recovered from a backup file. Therefore, acquiring data from this file can be important. Backup files do not contain applications (iOS version 4.0 and higher) music, movies, etc.

To add an iOS backup folder to a case, navigate to the iOS backup folder and select only the top-level directory of the iOS backup. A device's top-level directory has a 40-character UDID name value and has other similarly named folders inside.

Activate the checkbox for the iOS backup that is to be imported. If it is an encrypted backup, a lock icon will be displayed next to the backup name and the device will be deselected. Select the encrypted backup in the middle column, and a dialog window opens, prompting for the encrypted backup password that was in effect when the backup was made. Enter the password and click **Confirm Password**. Without the backup password, only ancillary data will be available for collection - media and some third-party application data.

Inspector does not attempt to crack this password, however there are several third-party applications available that do. For more information, see this topic provided by Apple: <http://support.apple.com/kb/ht4946>.

**Note:** The encrypted backup password is not the device's PIN code. The encrypted backup password is a password that a user has set in iTunes when backing up the iOS device to a computer.

In the middle portion of the Add Evidence window, an Evidence ID text box is shown, and this text box can be clicked and edited with an alphanumeric evidence ID for the iOS backup folder.

Choose the desired ingestion options and click **Start** when ready to begin the import.

**Note:** Because an iOS backup folder import contains only logical data, the backup folder does not contain unallocated space the way a bit-by-bit forensic image of the iOS devices would.

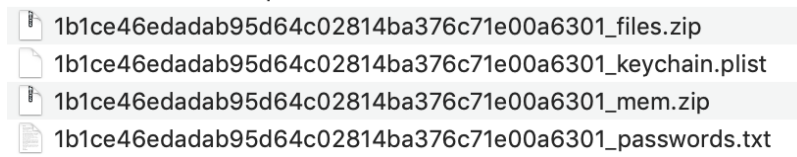
### Exporting and Importing iOS Backups from a Disk Image

If an iOS backup is included in an evidence item (e.g., a disk image) that is already part of the Inspector case, the iOS backup can be exported and then imported into the case. Once imported into the case file, the iOS backup will appear as a separate evidence item in the Component list.

Any available iOS backups contained in a selected evidence item can be found by navigating to the Actionable Intel view, then selecting **Device Backups** from the listed items. For more information, see [Actionable Intel View](#).

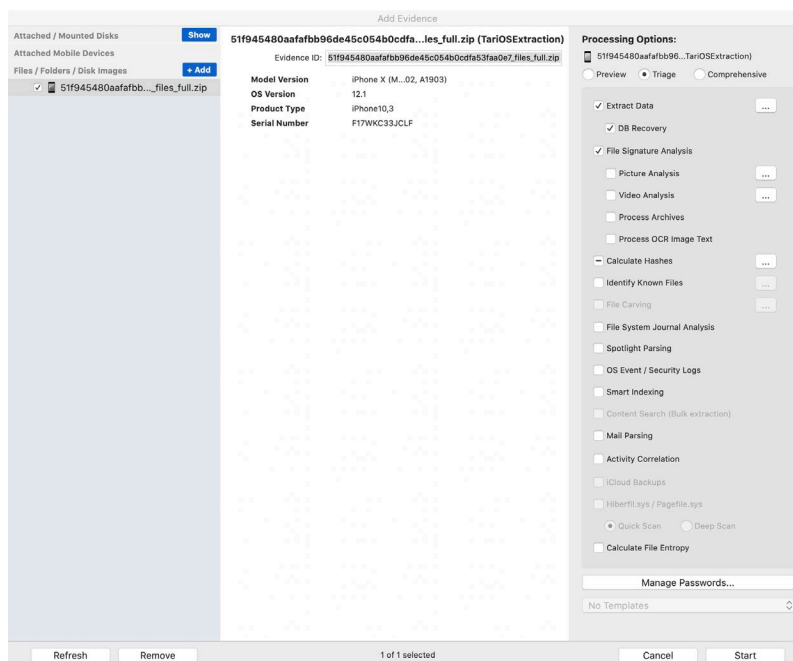
## Ingest GrayKey Images

Inspector can ingest and process Graykey images. Doing this provides access to the data in the images through parsing, and it also allows full filesystem analysis. GrayKey images are supplied as zip files.



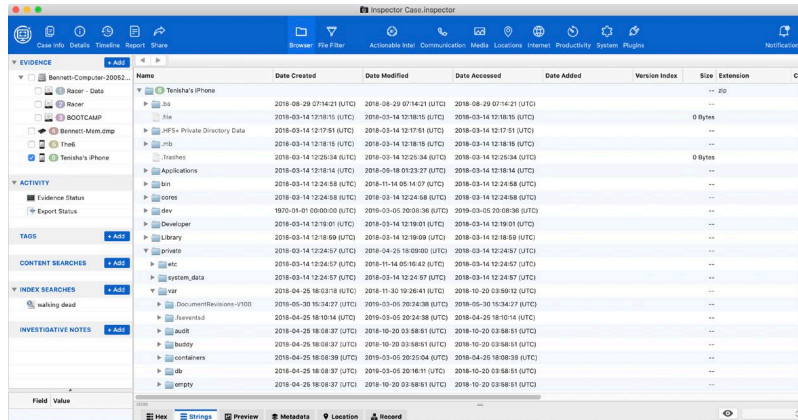
You can add each of these to Inspector by dragging and dropping them onto your case, or you can click **Add**.

When the Add Evidence window appears, choose the options and click **Start**.

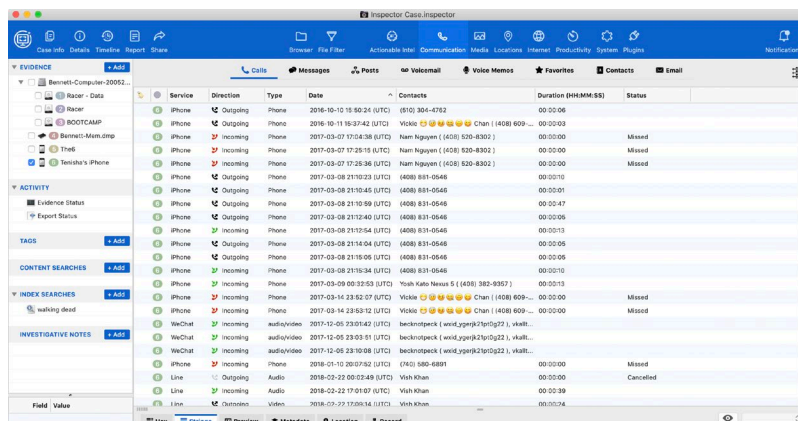


Inspector processes the GrayKey zip file just as if it were processing an iOS backup, except with much more data. This depends on which zip file you choose, since GrayKey provides these types.

- `<name>_files.zip` contains the entire file system dump.
- `<name>_backup.zip` is an iOS backup version.
- `<name>_mem.zip` lets you choose whether to bring it in as a simple zip archive so you can see the contents, or as a folder so you can do a full bulk extraction on it to get evidentiary items like IP addresses, email addresses, and so on.



Navigation through a GrayKey image looks just as if it came straight from the device itself.



## Adding a Memory File

Every bit of data being created, viewed, or destroyed goes through RAM, including all web-browsing activity, editing of documents, viewing of pictures, sending and receiving of network data, execution of applications, etc. Some types of artifacts only exist in RAM, and many types of ephemeral operating system artifacts are never stored to disk (e.g., what applications are currently running, what files and network connections are currently open, or what drivers are loaded). RAM artifacts can potentially tell examiners if malware, anti-forensics tools, or encryption software was running, if the machine had open network connections to known websites of interest, and/or what picture files a viewer application had open.

An in-depth study of memory forensics is outside the scope of this manual.

The process for adding a memory file is begun the same way as for adding any form of evidence to an Inspector case.

For more information, see [Adding Evidence to a Case](#).

Inspector automatically identifies a memory file and Processing Options are adjusted. You can perform a Quick Scan (default) or a Deep Scan. The Quick Scan option is faster and searches the most likely locations. Deep Scan takes more processing time and searches in additional locations less likely to yield content.

**Processing Options:**

☒ EFI System Partition (FAT32)

☐ Preview ☐ Triage ☐ Comprehensive

☒ Extract Data ...

☒ DB Recovery

☒ File Signature Analysis

☐ Picture Analysis ...

☐ Video Analysis ...

☐ Process Archives

☐ Process OCR Image Text

☒ Calculate Hashes ...

☐ Identify Known Files ...

☐ File Carving ...

☐ File System Journal Analysis

☐ Spotlight Parsing

☐ OS Event / Security Logs

☐ Smart Indexing

☐ Content Search (Bulk extraction)

☐ Mail Parsing

☐ Activity Correlation

☐ iCloud Backups

☒ Hiberfil.sys / Pagefile.sys

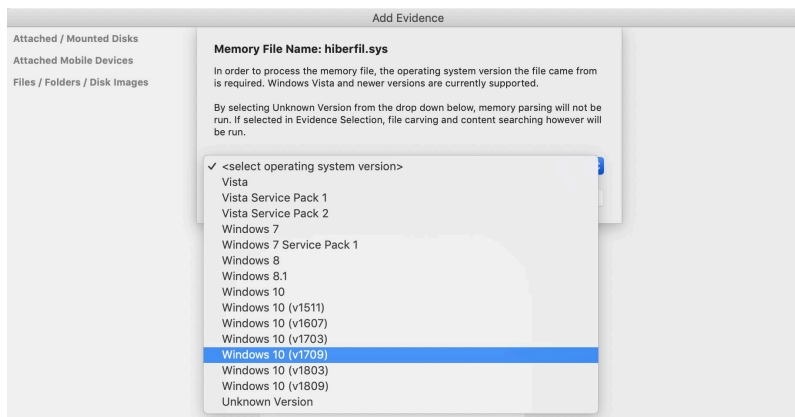
☒ Quick Scan ☐ Deep Scan

☐ Calculate File Entropy

Manage Passwords...

No Templates

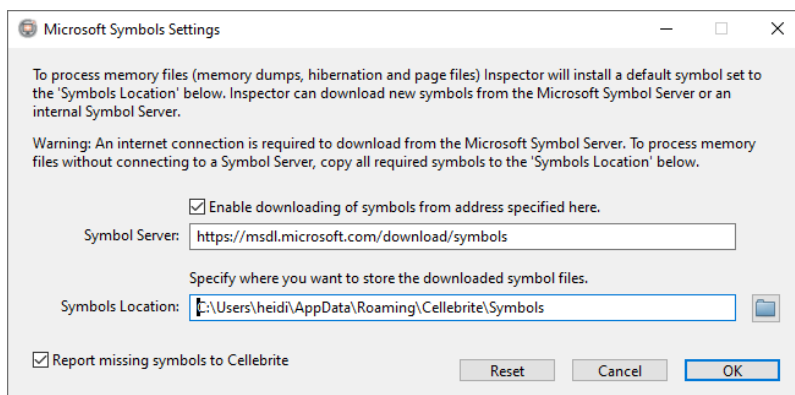
If attempting to add a *hiberfil.sys* (Hibernation) file, a separate window will open prompting for the Windows OS version that was used to create the file. Choose the operating system version from the drop-down menu and click **Confirm Version**. If you select **Unknown Version** from the drop-down menu, memory parsing will not be run. However, file carving and content searching can still be run from the Add Evidence window if desired.



**Note:** Inspector can also scan the volumes within a Windows disk image for *hiberfil.sys* (Hibernation) and *pagefile.sys* files, and if found, process these files as separate evidence items in the Evidence list. To do so, run the appropriate processing options on the volume. For more information, see [Adding a Disk Image](#).

## Microsoft Symbols

Inspector requires Microsoft symbols in order to process Windows memory files. If Inspector does not have access to these symbols, nothing can be extracted from memory files. These symbols are stored on the Microsoft Symbol Server, which can be accessed over the Internet. You can manage preferences for accessing Microsoft symbols from the Preferences window. For more information, see [Inspector Preferences or Options](#).



The Symbols Location field is the location where Inspector is set to install a default symbol set, and it is location where for any downloaded symbol files are saved. Selecting the folder icon allows you to choose a different location for symbols. Click **Reset**, and Inspector restores the Symbols Location field to the default path.



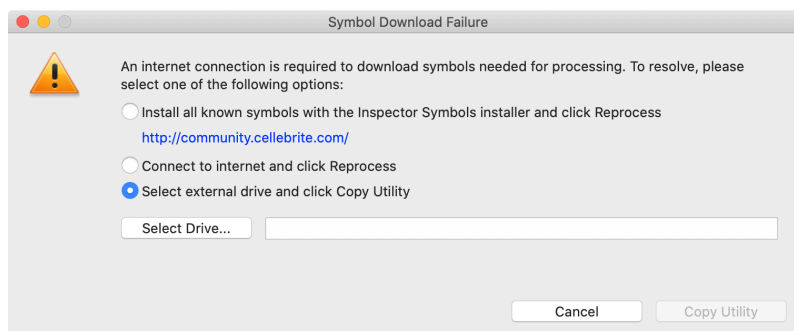
Inspector can download new symbols from the Microsoft Symbol Server or an internal server. By default, the checkbox is activated to enable downloading of symbols, and the Microsoft server address is selected. An Internet connection is required to download from the Microsoft Symbol Server. To disable automatic downloading of symbols, unmark the checkbox for **Enable downloading of symbols from address specified here**.

By default, Inspector sends anonymized data about the necessary symbols back to Cellebrite, so that we can consider including the symbols in our future symbol packs. Reporting can be disabled by unmarking the checkbox for **Report missing symbols to Cellebrite**.

To connect to an internal symbol server, change the address in the **Symbol Server** field.

To process memory files without connecting to a symbol server, copy all required symbols to the location shown in the **Symbols Location** field.

If you have disabled symbol downloading or you have no Internet connection, Inspector may fail when processing a memory file. In this case, if you right-click the error badge for the memory file and click **Show Errors**, a window appears offering these options.



1. Download and install the offline symbol pack from Cellebrite, which contains all of the currently known symbols. (In most cases this will be adequate.)
2. Connect to the Internet and reprocess.
3. Copy a utility to an external drive (such as a USB drive), which can then be connected to an Internet-connected computer and run. The symbols are downloaded to the USB drive. The USB drive is then connected back to the computer running Inspector, and the symbols are copied over. (To do this, click **Select Drive**, select the external drive, then click **Copy Utility**.)

## Analyzing Memory Files

After a memory file has been added to Inspector and processed with the desired processing options, the parsed contents can be analyzed. In the Browser view, files carved from the memory file are separated by type and then file type extension. Each file can be viewed within the appropriate Inspector view. For instance, if any pictures have been carved from the memory file, they can be viewed in the Media view.

Memory file artifacts can also be viewed within the Memory sub-view. On the toolbar, click **System > Memory**. For more information, see [System View](#).

When the examiner runs processing options on a memory file, Inspector uses a bulk extraction tool to perform content searches, scanning the evidence file for key items of interest. For more information, see [Bulk Extraction Searches on Memory Files](#).

## Adding a USB Attached Mobile Device

Inspector can logically acquire and process an attached iOS (i.e., iPod, iPhone or iPad) or Android device. The process for adding an attached mobile device is begun the same way as for adding any form of evidence to a Inspector case. For more information, see [Adding Evidence to a Case](#). Additional steps and considerations pertaining to mobile devices are discussed below.

### Settings for Android Devices

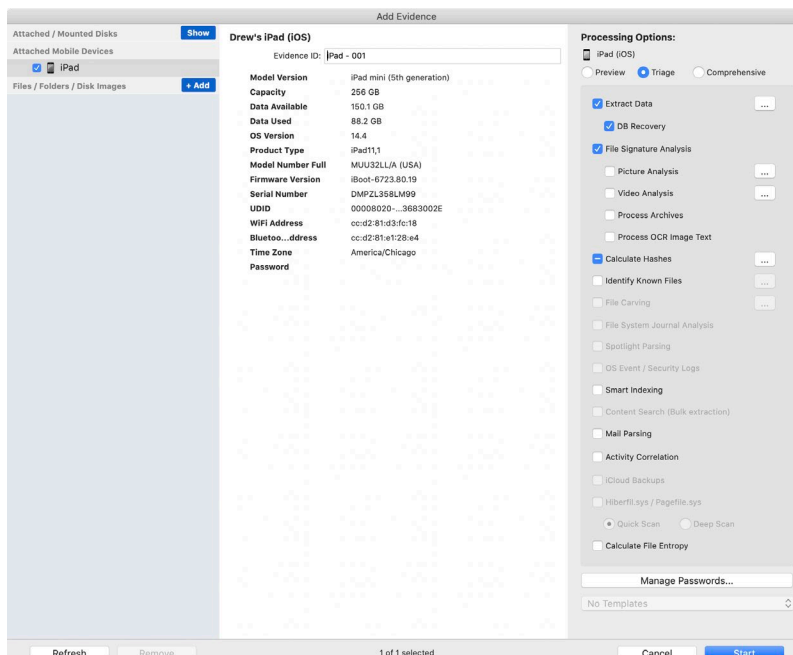
In order to have the analysis system recognize an Android device, make sure the Android device is unlocked, and that the USB debugging mode has been selected from the Developer options (or, on some devices, Development) in the device's Settings menu. The USB debugging option may have to be selected and unselected a few times on some Android devices.

**Note:** Newer Android devices may have the Developer option hidden. Go to **Settings**, select **About phone**, and tap **Build number** seven times. Then return to the **Settings** menu. Select the unhidden **Developer options** (or **Development**) and choose **Android debugging**. (The exact wording for these settings may vary slightly from one device to another.)

Once the device is in USB debugging mode, and the RSA key fingerprint has been created by tapping **OK**, it is sometimes necessary to change the mode of the device. In order to do this, swipe down from the top of the device screen and choose the **USB computer connection** option. From here, Media device (MTP), Camera (PTP), or Internet mode can be chosen. While Media device (MTP) is the most common mode, the user may have to try Camera (PTP) or Internet mode for the device to be recognized.

## Adding Evidence from a USB Attached Android or iOS Device

When a live Android or iOS mobile device is attached, and the PIN has been used to unlock the device, data can be acquired. The device will be shown in the Attached/Mounted Devices area. By highlighting the device, its information is revealed in the middle portion of the window.



When finished with the options in the Add Evidence window, click **Start** to start the data acquisition and processing. In the Component list select Evidence Status. Inspector begins acquiring and processing the data according to the options chosen. Disconnect the iOS device only after the acquisition is complete.

**Warning:** Never disconnect an iOS device during backup or acquisition.

## Additional Notes on Adding Mobile Devices to a Case

When an examiner adds a USB attached mobile device, Inspector acquires logical data (not a bit-by-bit forensic image acquisition) from an attached device and places the data into the case file. When iOS data is acquired using this option, Inspector leverages the iTunes API backup functionality. However, it is important to note that this acquisition is much more thorough than a simple iTunes backup. A special low-level connection is also established, and additional data not contained in a normal iOS iTunes backup is also acquired. This is the best method to use to acquire and examine logical iOS data when a physical image is not possible.

Because Inspector does not forensically image or jailbreak iOS devices, email is not acquired. But SMS/MMS messages, contacts, phone calls, voicemails, pictures, etc., are.

Acquiring data using this method may cause a case file to become quite large, depending on the size of the iOS device, so be sure the case is stored on media with the appropriate capacity.

It is best to disable wireless connectivity on mobile devices before acquiring data from them.

Some iOS applications may cause data acquisition or processing to fail. If this happens, quit and relaunch Inspector. The acquisition may continue successfully. If another failure occurs, remove the iOS device and re-add it to the case with different processing options selected. You can find debugging instructions and additional troubleshooting information in [File System Information](#).

If adding an Android device that is "rooted," ensure that the device's developer option for Root Access is set to Apps and ADB before beginning the collection. If this Root Access option is set to Apps Only, Inspector may not be able to properly interact with the device.

## Adding Other Attached Devices

An examiner may use Inspector to perform an analysis of attached devices. These include a mounted device such as a .dmg image, a Time Machine/Time Capsule image, an external FireWire or USB drive, or a mounted .E01 file. For more information, see [Appendix 2 - EWMounter](#).

The process for adding attached devices is begun the same way as for adding any form of evidence to an Inspector case. For more information, see [Adding Evidence to a Case](#).

**Important:** Be sure to have appropriate software-based or hardware-based write-blocking in place before attaching an evidentiary device to an analysis workstation.

## Adding a Mobilyze Case

Cases created and stored with Mobilyze, Cellebrite's mobile device triage tool, may be added to an Inspector case. Mobilyze has the potential to acquire some types of data that cannot be displayed within that application, yet will be viewable in Inspector, which is designed for more comprehensive analysis.

**Note:** Cases exported from Mobilyze as .zip files cannot be directly added to Inspector; they must first be unzipped.

To add a Mobilyze case to Inspector, follow the same process as for adding any form of evidence to an Inspector case. For more information, see [Adding Evidence to a Case](#).

In the left pane of the Add Evidence window, click **Add**. Navigate to the desired Mobilyze folder and click **Select**. The Add Evidence window recognizes the folder as a Mobilyze case and notes it as such in the middle pane.

When finished with the options in the Add Evidence window, click **Start** to begin adding the Mobilyze case to the Inspector case.

## Adding a Folder or File

You may add targeted or triaged evidence stored in individual folders or files to a case.

The process for adding a file or folder is begun the same way as adding any form of evidence to an Inspector case. For more information, see [Adding Evidence to a Case](#).

Inspector imports and processes the chosen evidence items, and they are displayed in the Evidence section of the Component list.

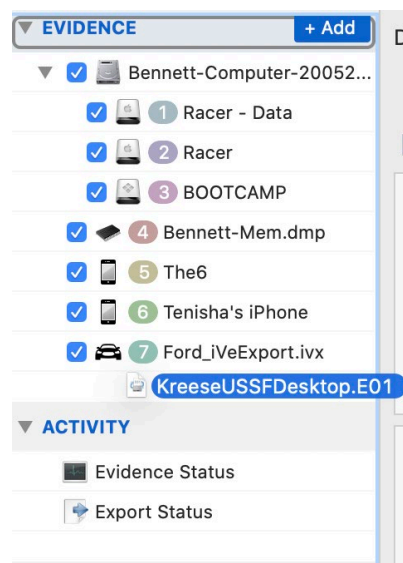
## Adding Evidence Using Drag and Drop

You can add data to a case in Inspector using the drag-and-drop method for these data ingestion options.

- Disk Image: Add a forensically acquired or virtual disk image (DMG, DD, VMDK, E01, Ex01, L01, S01)
- Folder: Add a folder and folder contents
- File: Add a file

For more information, see [Tags](#).

Select one of the above data source types from Finder and drag it onto the Component list. A border appears around Evidence. Drop the file onto the Component list and the Add Evidence window appears.



From this point, follow the same process as for adding any form of evidence to an Inspector case. For more information, see [Adding Evidence to a Case](#).

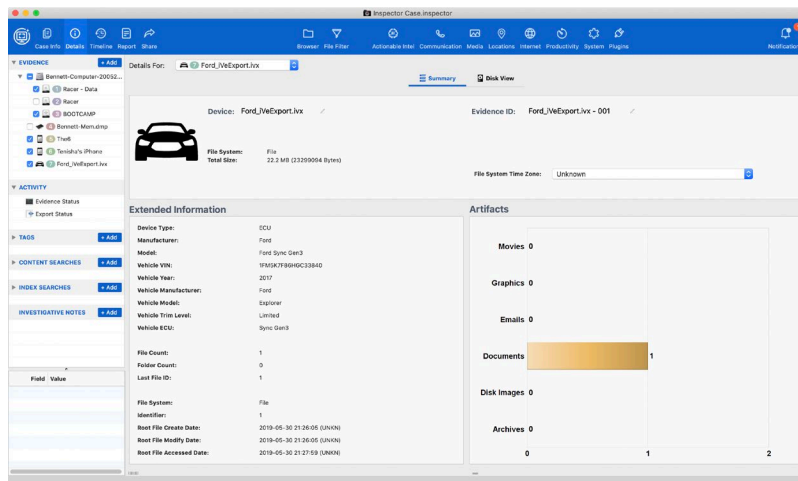
Inspector imports and processes the chosen evidence items, and they are displayed in the Evidence section of the Component list.

## Adding Berla iVe

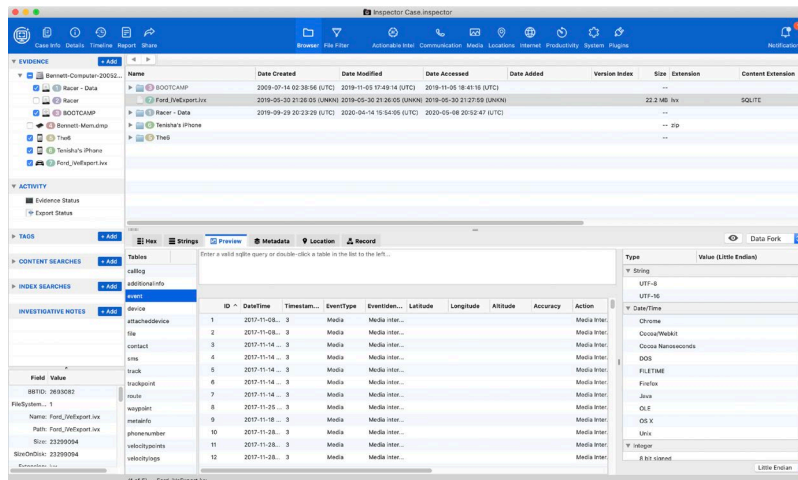
Working with Berla Corp, Inspector is capable of importing data exported from Berla iVe. Berla Corp is the industry leader in vehicle forensics. Vehicles contain a vast amount of data useful during an investigation. Data such as routes, vehicle events, location data, connected devices, and media can all be contained in computers in a vehicle. Once the data is acquired using the Berla iVe ecosystem, it is then imported into Berla's iVe forensic software. Berla Corp has added an option in iVe Desktop to export data to a .ixv database for import into Inspector.

Choose the .ixv file in the Add Evidence window.

Inspector ingests the .ixv database and processes the data.

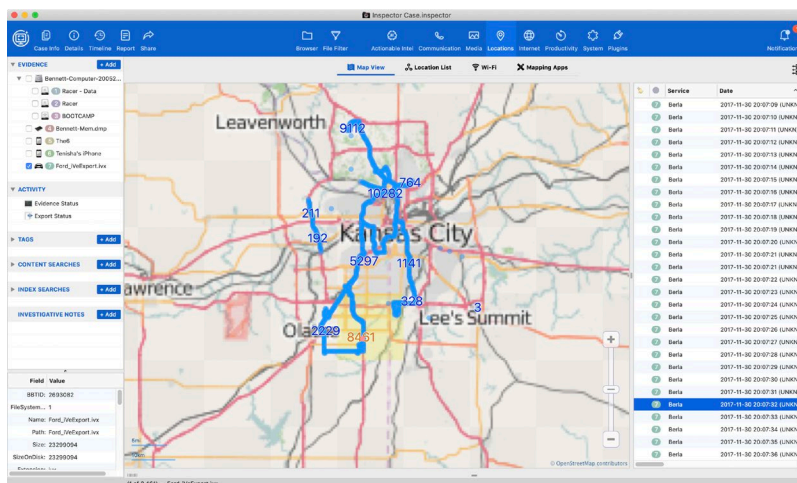


All of the data included in the .ixv database can be viewed from the Browser view, using the Preview tab in the File Content view.



Data is parsed into these areas in Inspector.

- Actionable Intel
  - Device Connections
  - File Knowledge (Recent Items)
  - Account Usage (Top Contacts)
- Communication (Calls, Contacts)
- Locations (Map View, Location List)
- System (System Log)



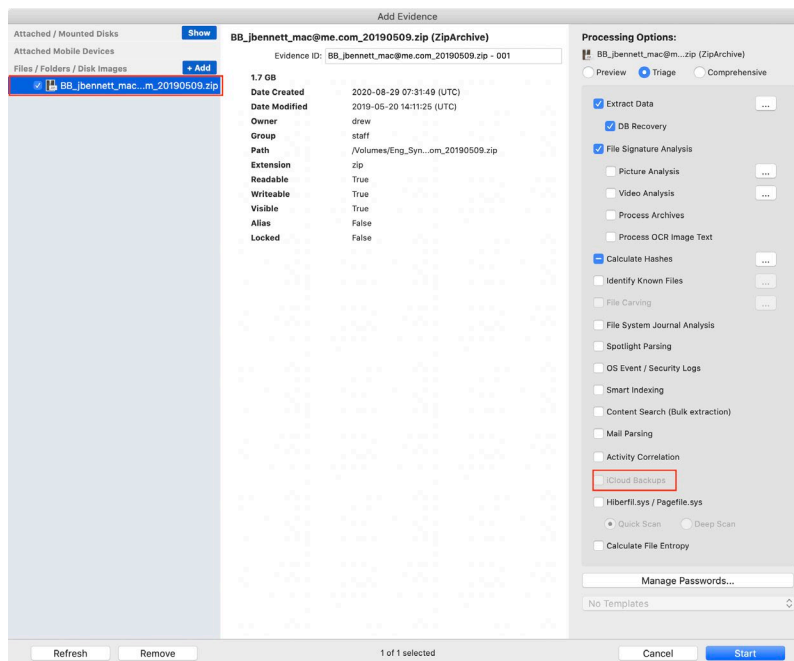
## Adding iCloud Productions

With the proper search authority, Apple provides data from a user's iCloud account using that person's Apple ID. A myriad of data can be stored in a person's iCloud account including multiple device backups. iCloud Production files from Apple are sent in an encrypted GPG format. These files must be decrypted prior to ingestion. If an examiner attempts to add encrypted GPG files, Inspector will display a prompt indicating the GPG file must be decrypted. Decryption of the GPG file results in a .zip file.

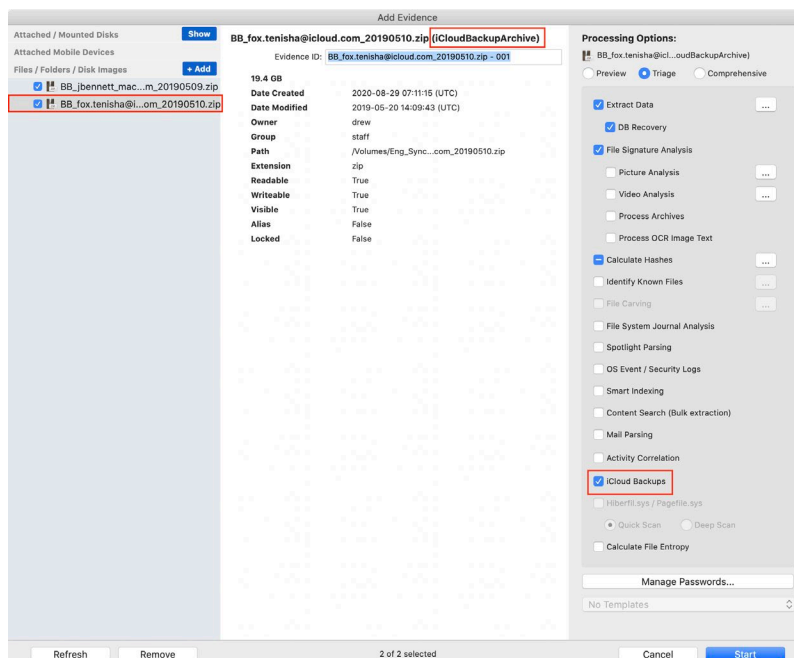
The process for adding an iCloud Production .zip file is begun the same way as adding any form of evidence to an Inspector case. For more information, see [Adding Evidence to a Case](#).

Ingesting data from iCloud production files relies on the formatting of these files. If Apple chooses to alter the format of the data in iCloud Production files, Inspector may cease to identify iOS device backups in the iCloud production files.

Some users do not store device backups in iCloud. Some iCloud Production files do not contain device backups. If this occurs, the iCloud Backups processing option will not be available for that set of iCloud Production files and Inspector will identify the file as a ZipArchive.

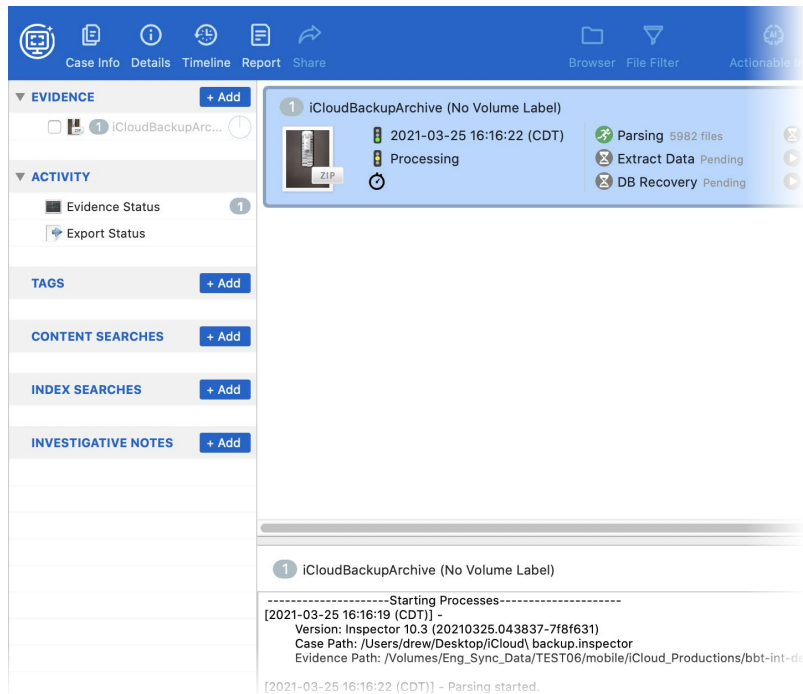


For iCloud productions containing iOS device backups, Inspector identifies the zip files as an *iCloudBackupArchive*. The device backups are detected, and the processing option iCloud Backups is available and will be automatically marked. Some iCloud accounts contain multiple backups for the same device and backups for different devices.

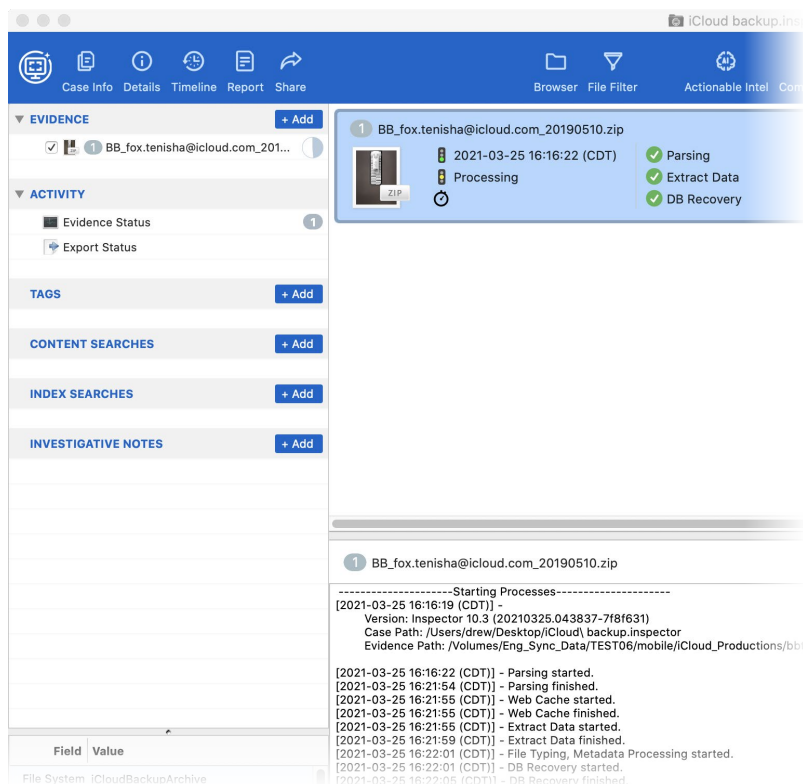




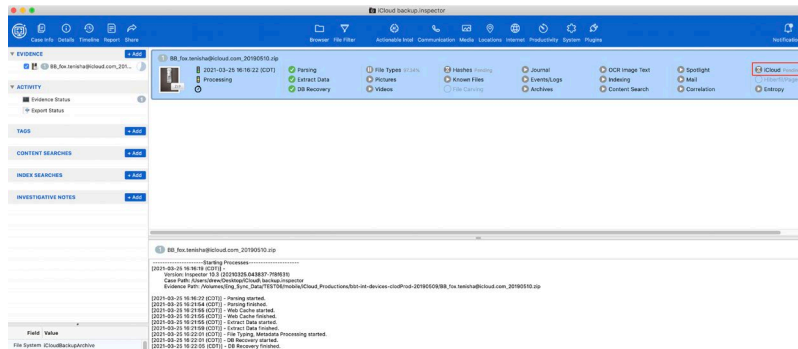
As the data is ingested, Inspector first identifies the zip file as *iCloudBackupArchive*. This can be seen in the Evidence Status section of the Component list.



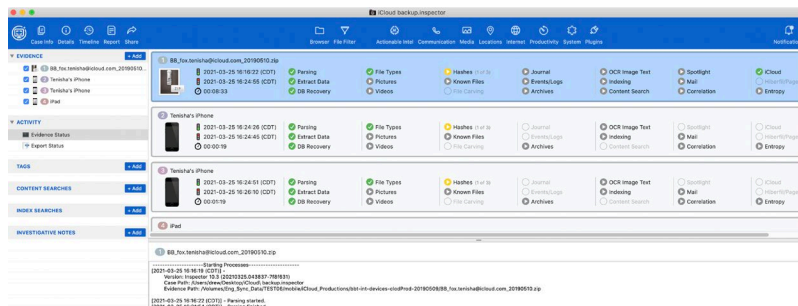
Once parsing completes, Inspector changes the Evidence Item name to the name of the .zip file.



Before iOS device backups are parsed, all other processing options must complete on the zip file. Once the iCloud process starts, the process on Evidence Status displays how many device backups there are.

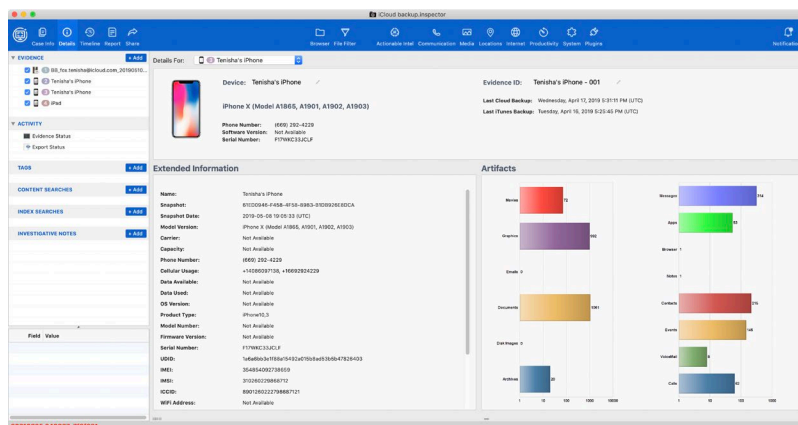


As the iOS backups are processed, they are added one at a time.



As Inspector parses the data stored in the backups, the temporary name *icloudfsstore* is applied to the backup. Once parsing begins on a backup, the name is changed to the Device Name of the iOS device.

As the iOS backups process, data on the backups can be viewed and examined.



## Adding UFED and Premium CAIS Acquisitions

Inspector supports UFED (segmented .zip) versions as well as Premium Cellebrite Advanced Investigative Services .dar formats for mobile device acquisitions.

**Note:** Only iOS images are supported.

When ingesting a UFED acquisition, point Inspector to the main .zip file for UFED extractions and the .dar file for Premium extractions.

If the iOS device is encrypted, you can select the device to enter the password in the Processing Options panel. You can find that password in the .ufd file accompanying the .zip file. If the password is validated the device is processed normally.

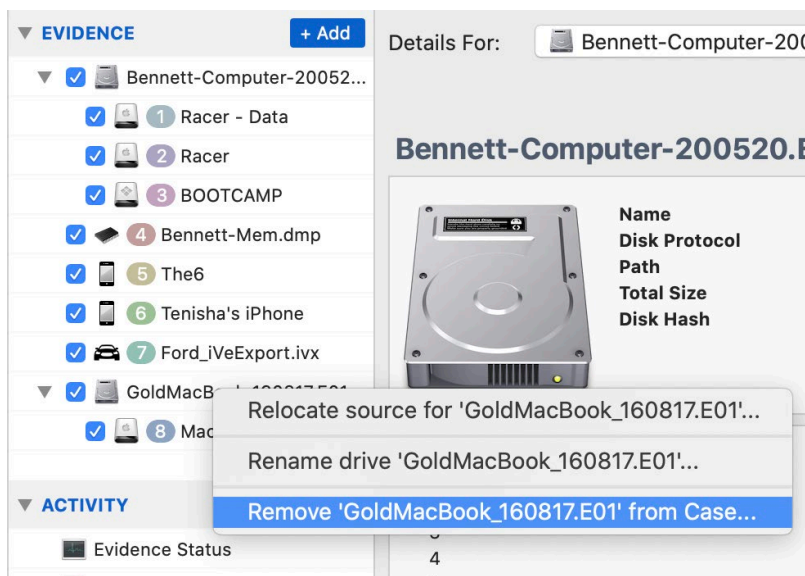
After Inspector parses a .zip file, the iOS file within the .zip file is parsed. You can see the additional item in the Evidence Status view and the Component list. The name of the iOS device changes during processing and is final when processing is complete.

You can investigate both the .zip file and the iOS device. The view depends on which evidence item you select.

## Remove Evidence from a Case

You may remove an evidence item from a case.

1. In the Component list under Evidence, right-click the evidence item to be removed.
2. Click **Remove <Item Name> from Case**.



3. In the confirmation dialog, click **Remove**.

**Important:** If you change your mind, you cannot simply add a removed evidence item back to a case. You must acquire and process it again.

## Move a Case File to a Different Computer

You can move a case file to a different computer for another examiner to look at. You must first create a case archive to move or copy it.

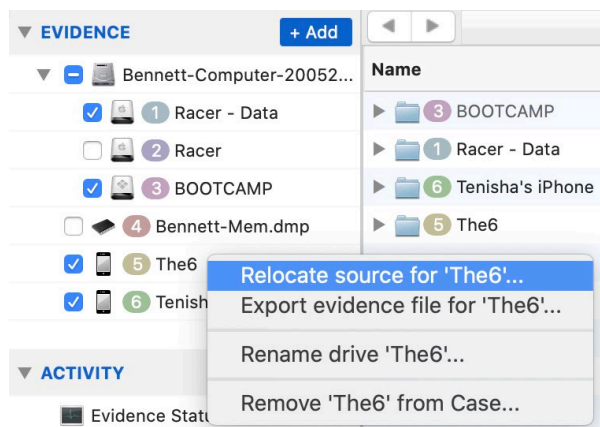
1. In the Case Manager window, select the case file.
2. Click **File > Create Case Archive**.
3. Choose the location to export the case file to and then click **Save**.
4. On the computer where the case should reside, open Inspector.
5. Click **File > Restore Case Archive**.
6. Navigate to the location of the saved archive from Step 3, select the archive folder, and then click **Open**.  
This message appears: **Would you like to restore this archive to a local case? Create a new case on this local system.**
7. Click **Local Case**.
8. Navigate to the location on this computer to restore this case file to, name the case, and then click **Save**.

When restoration is complete, the case file opens in Inspector.

## Relocating a Disk Image

**Before you begin:** Keep the Inspector case file on a local machine and not on a network resource, as some Inspector features may fail when the case file is accessed over a network.

If you move a disk image in a case to a new location on the same disk, Inspector automatically recognizes the image's new location. However, if you move the image to a new location on a different disk, such as a network share, Inspector does not recognize the disk image's new location. Therefore, <Disk Unavailable> appears next to the item in the Component list.



You must navigate to and select the disk image from within Inspector before data from the device is once again available for examination. In the Evidence section of the Component list, right-click or CTRL+click the device and then click **Relocate Evidence** from the context menu. In the navigation window, locate the disk image and select it. Inspector automatically links to the disk image in its new location and displays it in the Evidence section of the Component list.

## Exporting Mobile Device Evidence

You may need to export mobile device evidence to collaborate with another examiner or for e-Discovery purposes.

In the Component list under Evidence, select the mobile device evidence item to be exported. Right-click the device and click **Export Evidence File** from the context menu.

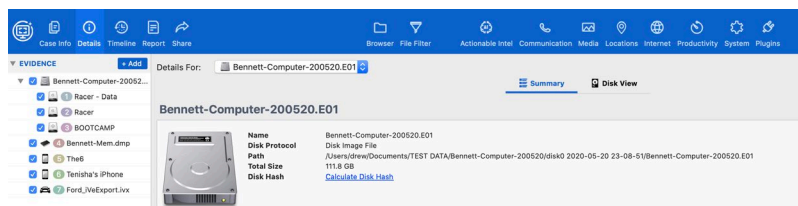
Select the destination for the exported file and click **Save**. You can monitor the progress of the export by selecting Export Status in the Component list.

The exported file for the mobile device evidence is named *Files.bbtar*.

**Important:** The exported file *Files.bbtar* can be renamed and the file extension .bbtar can be changed to .tar. However, if you ingest the exported file back into Inspector, the file extension must be .bbtar for Inspector to process it as a mobile device.

## Hashing and Verifying Forensic Evidence

To generate a disk image hash value, on the toolbar, click **Details** and then choose the dropdown option for the device. The **Calculate Disk Hash** link appears.



Click **Calculate Disk Hash**, and a Hash Types window appears. Select any or all of the desired hash type checkboxes.

As Inspector generates the hash values, a “Hashing” progress bar overlay appears in the Case Window. After hashing is complete, the hash values are displayed.

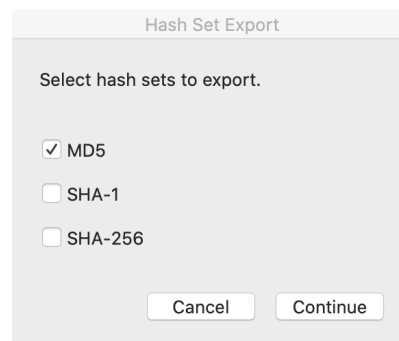
You can copy and paste text from the device description a text file or export the text to a spreadsheet or database file. Select any or all of the device description text, then use your operating system's shortcut keys to copy and paste the text into your text file. To export the selected text items to a tab-delimited or CSV file, select text items in the Content pane, then open Inspector's context menu and click **Export Selected Rows**.

You must manually verify (compare) hash values from a .dd or .dmg image, as these types of images (raw images) do not store hash values. However, because E01 hash values are stored in the E01 image itself, when you click Calculate Disk Hash, Inspector compares the generated E01 image file hash value to the hash values stored in the image file. If the hash values match, the word Verified- appears along with the generated hash values. Click the Calculate Disk Hash link any time to recalculate the disk hashes.

The known OS X and Windows hash sets have been updated to use hashes from [hashsets.com](http://hashsets.com). This increases the number of OS versions and total amount of hashes for hash comparisons, allowing you to filter out a larger number of unnecessary system files.

Inspector supports hash sets containing MD5, SHA-1, and SHA-256 hash values. Inspector allows you to import hash sets saved as text files as long as the file contains one hash value per line with each line separated by a carriage return. Inspector automatically identifies the type of hash value stored in the text file.

Custom hash sets created in Inspector are automatically saved in the .blhs format. Hash sets can be created containing MD5, SHA-1, SHA-256 or any combination of the three. Choose the hash types to be included in the hash set in the Hash Set Export window.



## Advanced Evidence Recovery

Inspector includes several disk and partition editing and recovery features. An examiner may specify sector size, edit or define hidden or missing partition parameters, import a partition as unallocated space, and create an .iso disk image file from a partition.

As outlined in the [Adding Evidence to a Case](#) topic, begin the process for adding any of these evidence items to a case.

- Disk Image: Add a forensically-acquired or virtual disk image (DMG, DD, VMDK, E01, Ex01, L01, S01, AFF4)
- Selected Image File: Add the selected image file or virtual machine file located in a Component list device (available only when an image file or VM file is selected)
- Encrypted iOS Disk Image: Add a forensically-acquired third-party iOS disk image with proprietary encryption enabled (such as Lantern Lite, etc.)
- Other Attached Device: Add a mounted device such as a .dmg image, a Time Machine / Time Capsule image, an external FireWire or USB drive, or a mounted .E01 file (EWMounter)

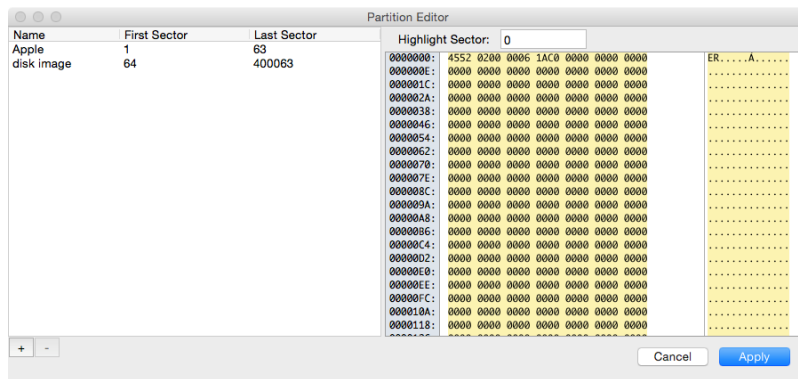
## Manually Setting Disk Sector Size

In the Add Evidence window, open the context menu from the selected disk or partition, and then click **Set Disk Sector Size**. The Disk Sector Size window appears. In the **Sector Size** field, type the appropriate sector size and click **Set**. Inspector applies the new sector size.

**Note:** Most disks use a sector size of 512. Certain Advanced Format disks with a 4K Native (4Kn) label, as well as newer PCI-e NVMe solid state drives, use a sector size of 4096.

## Editing a Partition

To recover a deleted or missing partition, in the Add Evidence window open the context menu from a disk or partition, and then click **Edit Partitions**. The Partition Editor window appears.



To change an existing partition's definition, on the left side of the Partition Editor window under the First Sector and/or Last Sector column, double-click the partition's current sector definition. An editable text box appears. Type the desired sector definition and click anywhere in the Partition Editor window to escape the text box. The new first and last sector definition displays.

To highlight a specific sector, at the top of the Partition Editor window in the **Highlight Sector** field, type a sector number. Inspector jumps to the chosen sector and highlights the entire sector in yellow.

## Defining a Deleted or Missing Partition

To define a deleted or hidden partition, in the lower left corner of the Partition Editor window, click **+** (**add**). A New Partition <partition #> entry appears in the partition list. To define the new partition's first and last sectors, under the First Sector and Last Sector column, double-click on the zero. An editable text box appears. Type the desired sector definition and click anywhere in the window to escape the text box. The new partition's first and last sector definition displays.

To remove an existing partition, select a partition from the partition list and in the lower left corner of the Partition Editor window, click **-** (**remove**). The partition is removed from the partition list. Once all partition definitions are as desired, in the lower right corner of the Partition Editor window, click **Apply**. Inspector applies the new partition definitions.

## Importing or Processing a Drive or Partition as Unallocated Space

When an item is selected in the left pane of the Add Evidence window, all its partitions are displayed in the middle pane. Partitions with recognized file systems that can be imported into Inspector are displayed with a checkbox to allow selection. However, any partition, whether it has a checkbox or not, may be imported as unallocated. Open the context menu from the partition and select **Import Partition as Unallocated**. Select **Custom** in the right pane and **Carve Unallocated** becomes an available option.

Attached disks in the left pane can also be imported as unallocated in the same fashion. From the context menu, select **Import as Unallocated**.

In the Add Evidence window, mark the checkbox for **Carve Unallocated** and click its corresponding ellipsis button to specify the unallocated file types to include in the recovery.

**Note:** If you open the context menu from a partition that is currently set for adding to the case as unallocated, **Import Partition Normally** is an available option in the context menu.

## Creating an .iso Disk Image from a Partition

If a disk image partition contains an unsupported file system format (such as ZFS), you may create an .iso image from the partition and examine it with a third-party forensic analysis tool. In the Add Evidence window, open the context menu from a partition and select **Create ISO from Partition**. The Creating ISO window appears.

In the **Start Sector** and **Sector Count** fields, define the partition start sector and the partition's total sector count, respectively.

To determine the number of sectors in a partition if the number is unknown, click **Cancel** to dismiss the Creating ISO window. In the Add Evidence window, open the context menu for a disk or partition and click **Edit Partitions**. The Partition Editor window appears. Locate the partition in the partition list and subtract the number in the First Sector column from the number in the Last Sector column and add one. The resulting number is the partition's total sector count. In the Add Evidence window, open the context menu from a partition and click **Create ISO from Partition**. The Creating ISO window appears.

In the **Start Sector** and **Sector Count** fields, define the partition start sector and the number of sectors in the partition, respectively. To create the .iso disk image file, click **Start**. Provide a name and destination location for the new .iso disk image and click **Save**. The .iso disk image is saved.

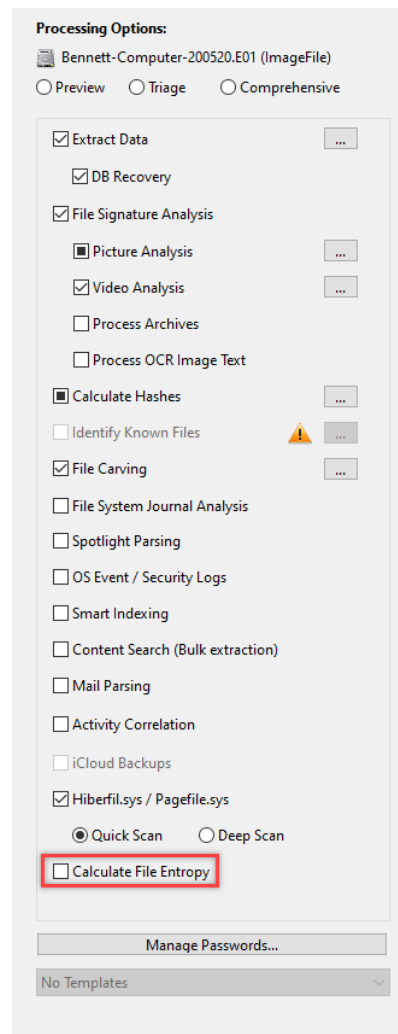
**Note:** You may use these evidence recovery features in tandem. For instance, if you discover a deleted or missing NTFS partition, the partition may be recovered using the Edit Partitions feature and exported for further examination to an .iso disk image using the Create ISO from Partition feature.



## File Entropy

With Inspector, you can calculate byte stream entropy per file, which can aid in discerning between items that are more likely to be encrypted versus those which are not. Entropy values range from 0 to 1, with values closer to 1 denoting items that are more likely to be encrypted.

You can process file entropy when adding an evidence item to a case. In Processing Options, mark the checkbox for **Calculate File Entropy** before you click **OK**.

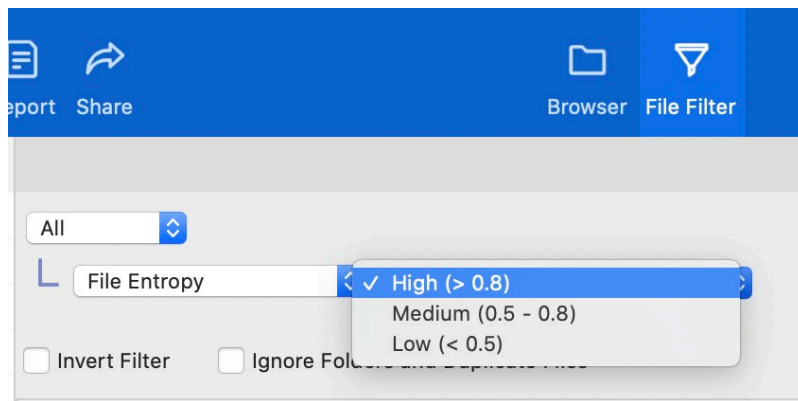


File entropy may also be processed after adding the evidence item to a case. Select an evidence item under Evidence Status in the Component list and click **Run** (or **Rerun**) next to **Entropy**.

Entropy is available as a sortable column for display in the Browser and File Filter views.

| Root               |                  |
|--------------------|------------------|
| Name               | Entropy          |
| 2015-11-24-074337  |                  |
| .mtm.private.plist | 0.68336509518773 |
| .Spotlight-V100    |                  |
| net                |                  |
| home               |                  |
| .fsevents          |                  |
| fsevents-uuid      | 0.46044279530415 |
| fc00759583d7a73a   | 0.61962065309746 |
| fc0075957efb89e0   | 0.62415171806813 |
| 00000000004b24c2   | 0.62681106787096 |
| fc0075957ee0f43a   | 0.62744119175234 |
| 00000000004b667e   | 0.62811936120954 |
| 00000000004a6982   | 0.63169078978097 |
| 000000000073f6fa   | 0.63472945272711 |
| fc007595841baf4f   | 0.64976405479731 |
| fc007595842ba37c   | 0.65383466324866 |
| fc007595842a44e7   | 0.65517257562704 |
| fc00759583f7c3de   | 0.65589578060977 |
| fc007595841c5808   | 0.65798503824144 |

File entropy is also available as an individual file filter in the File Filter view.



The File Entropy filter has these option modifiers.

- High (> 0.8)
- Medium (0.5 - 0.8)
- Low (< 0.5)

## Timeline View

The Timeline view lets you access more information from one place. It responds quickly, even with many items in a case file, and allows you to easily focus on all activity during a time period you specify. You can see and sort by all timestamps for each artifact in the Timeline view. You can also see the file path, so you can easily view the file in the File Browser view and investigate further. You can tag items in the Timeline view just as you would in other views within Inspector.

To open the Timeline view, click **Timeline** in the toolbar.

This chapter provides these topics about the Timeline view.

- [Time Scale](#)
- [Artifacts in Timeline](#)
- [Timeline Details](#)
- [Additional Timeline Features](#)

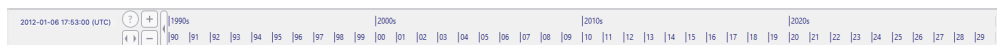
## Time Scale

To open the Timeline view, click **Timeline** in the toolbar.

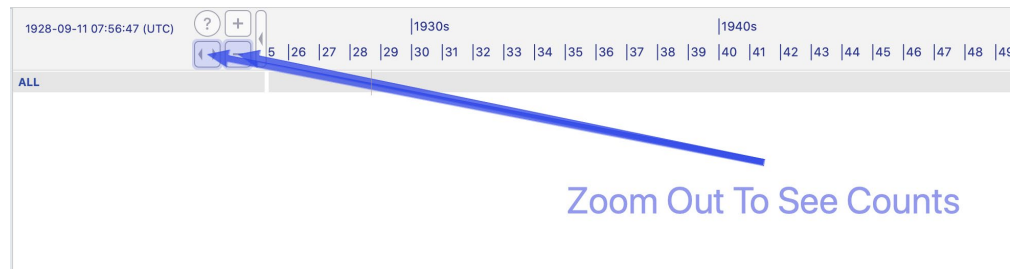
The time scale is the main navigation and display area for the time period currently in view. By default, the time scale centers its visible date range on the years between 1990 and 2024. You can move the visible timeframe, and thus changes the time period being viewed and the artifacts listed in the artifacts section. The scale can not be moved to a date before 1900, nor can it be moved to a date more than 20 years after the current date. These are the control buttons for timeline navigation.

- **?**, in the top left, is interactive help for the timeline.
- **+**, to the right of the help button, zooms in on the timeline.
- **-**, below the + button, zooms out on the timeline.
- **<>**, below the help button, returns to the original view if you are zoomed in or out too far.
- Two buttons on either edge of the timeline scroll the time view left or right. You can also use your mouse to click and drag the time scale left or right.

As you move the mouse along the histogram area, a thin grey line shows where in the timeline the current navigation is, and a corresponding date and time appears to the left of the navigation buttons.



You are notified if the time scale moves to a time where no data is visible. In the extreme example below, the date range visible in the time scale is between 1925 and 1949, and there are no artifacts during the time period. The help shows that you need to zoom out and change the date range to see any artifacts.



## Artifacts in Timeline

To open the Timeline view, click **Timeline** in the toolbar.

Below the time scale, you can see where artifacts fall within the timeline. A histogram shows where the most artifact activity falls within the visible date range. The larger the histogram, the more data that exists for that period.

In addition to all the artifacts in the case, the Timeline view shows categories for the artifacts. All categories show by default; you can hide any of them as appropriate. These categories are the same you see in the Inspector case. As you move the mouse along the histogram area, a thin grey line shows where in the timeline the current navigation is.



The categories list to the left of the histogram area does not move when you change the time scale. This helps you stay oriented when viewing artifacts over time. It does update to show category information for the time period currently selected. To see more details for a specific time, you can click and drag left or right to highlight the timeframe that needs to be zoomed in on.



|                 |         | 2011 |   |   |   |   |   |   |   |   |    |    |    | 2012 |   |   |   |   |   |   |   |   |    |  |  |
|-----------------|---------|------|---|---|---|---|---|---|---|---|----|----|----|------|---|---|---|---|---|---|---|---|----|--|--|
|                 |         | 1    | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1    | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |  |  |
| ALL             | (24.0k) |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| Files           | (22.4k) |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| ▼ Communication | (283)   |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| Call            | (4)     |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| Message         | (279)   |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| ▼ Internet      | (973)   |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| Bookmark        | (3)     |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| Cookie          | (834)   |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| Downloads       | (4)     |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| History         | (129)   |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| Top Sites       | (3)     |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| ▼ Productivity  | (37)    |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| Calendar        | (33)    |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |
| Note            | (4)     |      |   |   |   |   |   |   |   |   |    |    |    |      |   |   |   |   |   |   |   |   |    |  |  |

To see the Timeline view, click **Timeline** in the toolbar.

| #  | Type      | Content                   | Modified | Name                 | Participants         | Subject | Content                                        | Path                                        |
|----|-----------|---------------------------|----------|----------------------|----------------------|---------|------------------------------------------------|---------------------------------------------|
| 0  | message   | 2015-12-17 17:37:52 (UTC) |          | Step (step@msn.com)  | Step (step@msn.com)  |         | Just what you say my man                       | Users\jshen\Documents\Chats\2015-12-01\Step |
| 1  | message   | 2015-12-17 17:38:17 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) new online                | Users\jshen\Documents\Chats\2015-12-01\Step |
| 2  | message   | 2015-12-17 17:38:17 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | -step@msn.com is now online                    | Users\jshen\Documents\Chats\2015-12-01\Step |
| 3  | message   | 2015-12-17 17:38:36 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step hanging at home      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 4  | message   | 2015-12-17 17:38:48 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | what's up with you                             | Users\jshen\Documents\Chats\2015-12-01\Step |
| 5  | message   | 2015-12-17 17:39:03 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | nothing, can't sleep                           | Users\jshen\Documents\Chats\2015-12-01\Step |
| 6  | message   | 2015-12-17 17:39:53 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | playing with my new tooth, what you been doin  | Users\jshen\Documents\Chats\2015-12-01\Step |
| 7  | message   | 2015-12-17 17:40:13 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 8  | message   | 2015-12-17 17:40:54 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 9  | message   | 2015-12-17 17:40:54 (UTC) |          | Step (step@msn.com)  | Step (step@msn.com)  |         | What the fuck! what message session started    | Users\jshen\Documents\Chats\2015-12-01\Step |
| 10 | message   | 2015-12-17 17:40:54 (UTC) |          | Step (step@msn.com)  | Step (step@msn.com)  |         | But it's not mine, I'm not the one who started | Users\jshen\Documents\Chats\2015-12-01\Step |
| 11 | message   | 2015-12-17 17:41:02 (UTC) |          | Step (step@msn.com)  | Step (step@msn.com)  |         | where did you get that                         | Users\jshen\Documents\Chats\2015-12-01\Step |
| 12 | message   | 2015-12-17 17:41:02 (UTC) |          | Step (step@msn.com)  | Step (step@msn.com)  |         | It's not mine, I'm not the one who started     | Users\jshen\Documents\Chats\2015-12-01\Step |
| 13 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 14 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 15 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 16 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 17 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 18 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 19 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 20 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 21 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 22 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 23 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 24 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 25 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 26 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 27 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 28 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 29 | message   | 2015-12-17 17:41:02 (UTC) |          | Self (jshen@msn.com) | Self (jshen@msn.com) |         | Self (jshen@msn.com) step                      | Users\jshen\Documents\Chats\2015-12-01\Step |
| 30 | message</ |                           |          |                      |                      |         |                                                |                                             |

To zoom in on the timeline to a specific timestamp for an item, select the specific timestamp for that item in the details list, open the context menu, and click **Reveal > Reveal <timestamp> in Timeline**. This lets you quickly see what other activities may have occurred in proximity to that activity on the timeline.

## Additional Timeline Features

To see the Timeline view, click **Timeline** in the toolbar.

To see artifacts from the details view of the timeline in their native view of Inspector, open the context menu for the artifact, then click **Reveal > Item in Native View**. The view then redirects to the appropriate location with the selected artifact highlighted.

Conversely, to see where a piece of evidence lies in correlation with other items in the Timeline view, open the context menu for that item, and then click **Reveal > Reveal <Item Name> in Timeline**, where <Item Name> is the name of the selected item.

## Browser View

In Inspector, the Browser view lets you navigate a device or device partition file system similar to using Finder on a Mac computer or File Explorer on a Windows computer.

In the Component list, select a device or device partition, and on the toolbar, click **Browser**. In the Content view, expand a folder to see a hierarchical file list. Collapse the folder and the hierarchical list is hidden. Double-click on a folder to display only the contents of that folder.

[illegible]

You can quickly show or hide all folders within the parent folder. On a Mac computer, press **OPT**, and on a Windows computer press **ALT** while you click to expand two levels of child folders, or close all folders within the parent folder.

The Browser view displays file timestamps, sizes, extensions, and hash values. Select a column heading to sort files by the column attribute. To calculate and display folder size (including folder contents), right-click or CTRL+click on the folder and select **Calculate Size** from the contextual menu. Inspector calculates the folder size and displays results in the Size column. You may calculate folder size for the root-level folder or any folder in the file system.

To search folder contents, right-click or CTRL+click on a folder and select **Search Contents** from the contextual menu. Inspector switches to the Search view. The folder search path is automatically added to the search partition list and selected. For more information, see [Search](#).

At the top of the Content pane on the navigation bar, select the tabs to move to that location on the filesystem. Or you can use the arrows to the left of the tabs to go back to the previous location or forward to the most recent location. These arrows function as a historical navigation, not as a simple back and forward in file hierarchy.



The highlighted tab indicates your current location within the directory structure.

Select a file and at the top of the File Content view, scroll through Hex, Strings, Preview, Metadata, and Record to view file content in various ways. If a file has geolocation data, click **Location** to see a map displaying the file's GPS coordinates. For Mac computers only, you can click **Quick Look** (eye button) or press SPACEBAR to see the file rendered in a similar manner as the file's native creator application. For more information, see [File Content View](#).

In the Component list, select a previously processed unallocated (carved file) partition. A list of files recovered from unallocated space appears.

## Working with Columns

To change the visible columns settings, click **View > Adjust List Columns**. You can show or hide each item in the list marking or unmarking its checkbox. You can also reorder items in this list by dragging and dropping each item in the list to the appropriate order. When you have finished making changes, click **Apply Changes**. The columns now appear in the specified order.

To return columns to the way they were displayed by default, click **View > Adjust List Columns**. Click **Reset List to Defaults**, then click **Apply Changes**.

**Note:** Column options vary depending on which view is selected, and Inspector applies column option settings to each view independently.

When you export data using the Export Selected Rows feature, Inspector only exports the data in the displayed columns; data in the hidden (unmarked) columns is not exported.

The exception to this rule is the Contacts subview in the Communication. From this subview, all fields of the contact data, including those seen in the right pane, are included in exports. In most views that contain columns, clicking on a column header toggles between sorting by that column in ascending or descending order. A single arrow in the column header denotes a primary sort, as well as indicating the direction (up for ascending or down for descending). You can add a secondary sort by pressing SHIFT while you click a second column header. A set of double-arrows denote a secondary sort. You can remove a secondary sort by clicking a column of choice for primary sorting.

| Date Modified ^           | Date Accessed ∨           |
|---------------------------|---------------------------|
| 2014-03-24 14:50:47 (UTC) | 2017-11-29 18:50:15 (UTC) |
| 2015-06-11 22:36:40 (UTC) | 2015-06-11 22:36:40 (UTC) |
| 2015-06-11 22:55:04 (UTC) | 2015-06-11 22:55:04 (UTC) |
| 2015-06-11 22:55:11 (UTC) | 2015-06-11 22:55:11 (UTC) |
| 2015-06-11 22:55:11 (UTC) | 2015-06-11 22:55:11 (UTC) |
| 2015-06-11 23:46:27 (UTC) | 2016-12-08 14:48:33 (UTC) |
| 2017-11-30 13:11:01 (UTC) | 2016-12-08 14:48:33 (UTC) |
| 2016-06-24 10:51:10 (UTC) | 2016-06-24 10:51:10 (UTC) |
| 2016-10-26 14:13:53 (UTC) | 2016-10-26 14:13:53 (UTC) |
| 2017-09-01 01:09:23 (UTC) | 2017-09-01 01:09:23 (UTC) |
| 2017-10-03 00:36:27 (UTC) | 2017-10-03 00:36:27 (UTC) |



## Type-Down in List Views

In views that are based on list boxes, such as the Browser view, Communications views and so forth, you can type a letter (such as C), to immediately see the first item that begins with the letter C. If there is a secondary sort, the action is done only on the primary column.

## Special Fonts and Icons in Browser View

| Name                                         |
|----------------------------------------------|
| ▼ Temporary Internet Files                   |
| ▼ Content.IE5                                |
| container.dat                                |
| ▶ FSPMEXNZ                                   |
| ▶ Q4GFJBB7                                   |
| ▶ TA7C8ZSV                                   |
| ▼ ZD05JXM7                                   |
| <del>031-18696.English[1].dist</del>         |
| <del>031-36011.English[1].dist</del>         |
| <del>AppleApplicationSupport[1].msi</del>    |
| archive_full_BD_affiliates_wetabs_8[1].7z    |
| comment-delete-normal[1]                     |
| <i>current_BD_affiliates_wetabs_8[1].txt</i> |
| dtz[1]                                       |
| favicon[1].ico                               |

For NTFS and FAT volumes, Inspector scans the MFT for records of files and folders that no longer exist in the active file system.

Files and folders with sectors on disk that still contain data are shown in *red italic* font in the Browser view, indicating the file or folder was deleted but the space it was occupying has not yet been overwritten.

Files and folders with sectors on disk that are empty or that belong to another file are shown in ~~gray strikethrough~~ font, indicating the file was deleted and the space has been overwritten.

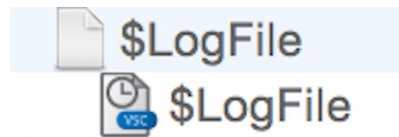
Gray font without strikethrough denotes that a file or folder has a hidden attribute set by the operating system. This means the file or folder is hidden from a user during regular browsing.

For Windows volumes, Inspector shows an ADS icon for a file with an alternate data stream.

## Volume Shadow Copies

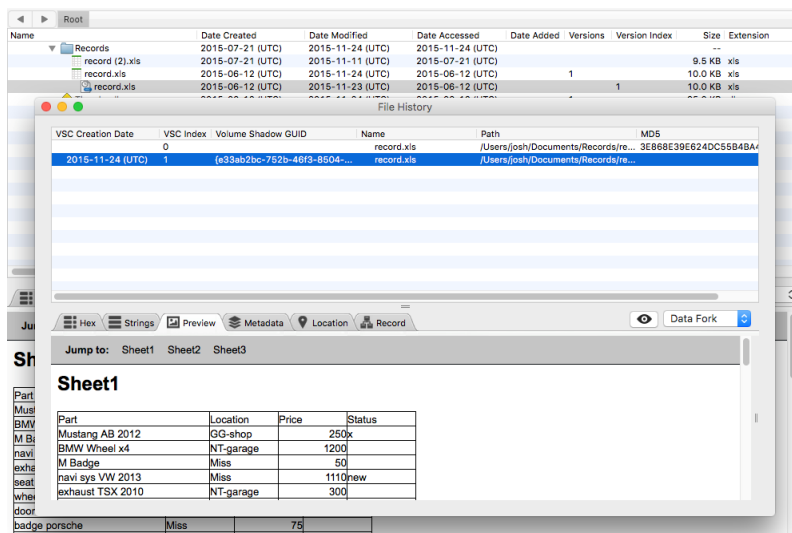
Volume Shadow Copy (VSC) data from Windows Vista to present is parsed in Inspector. VSC allows users to create a snapshot backup of their system. From a forensic standpoint, these backups may be important because they may contain files that the user believes was deleted. Also, VSC offers a means of saving versions of a file. Comparing file versions between the active file system and VSCs may reveal items changed between backups. Using Inspector, you can review the contents of VSCs in multiple ways, including viewing them within the same file paths as seen on the original user's computer.

For Windows volumes, Inspector displays a VSC version of a file with a VSC icon. For example, the upper file is the version from the active file system, while the lower file is a version from a Volume Shadow Copy.










**Note:** For the contents of a Volume Shadow Copy to be parsed and displayed, advanced processing options must first be run on the volume. For more information, see [Adding a Disk Image](#).

In either the Browser view or File Filter view, double-click any file that is, or has, a Volume Shadow Copy version, and a separate File History window appears. In this window all Volume Shadow Copy versions of a file can be further analyzed.






In the Browser view, files that exist in a Volume Shadow Copy but not in the parent volume are shown in *red-strikethrough-italic* font, indicating the file was deleted from the active file system but a version remains in one or more Volume Shadow Copies.

| Name                                                                              |                                        |
|-----------------------------------------------------------------------------------|----------------------------------------|
| ▼                                                                                 | workingcopy                            |
|  | audi-b8-a4-a5-black-trunk-emblem-4.jpg |
|  | bmwtires.jpg                           |
|  | golf-r-19-inch-alloy-glr4037-2.jpg     |
|  | porsche_912_1966_hood.jpg              |
|  | Thumbs.db                              |
|  | wheels.jpg                             |
|  | <i><del>lock.BMW_Wheels.doc#</del></i> |

**Note:** When viewing a list of Volume Shadow Copy versions of a file, it is possible to see more than one variant for a given VSC Index value. For example, there may be two records shown with the VSC Index value of '3,' one in regular black font and another in *gray-strikethrough*. The extra variant would represent an MFT record of an older version of the file. Inspector parses out the record and displays the metadata for that record, but the original file is gone and replaced (hence the *gray-strikethrough*). As such, the MFT for Index 3 would have two records for the file.

To see only a single Volume Shadow Copy's data, select the desired Volume Shadow Copy in the Component list.

|                                                                                     |                                                                                     |                                                                                     |                   |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------|
| ▼                                                                                   |  |  | BOOTCAMP          |
|  |  | 5                                                                                   | BOOTCAMP (Active) |
|  |  | 6                                                                                   | BOOTCAMP (VSC 1)  |

When viewing a specific Volume Shadow copy, only Internet data, media, communications, Actionable Intel view data, etc. related to that Volume Shadow Copy are seen in the various views in Inspector. For more information, see these topics.

- [Content Keyword Searches](#)
- [Individual File Filter Options](#)

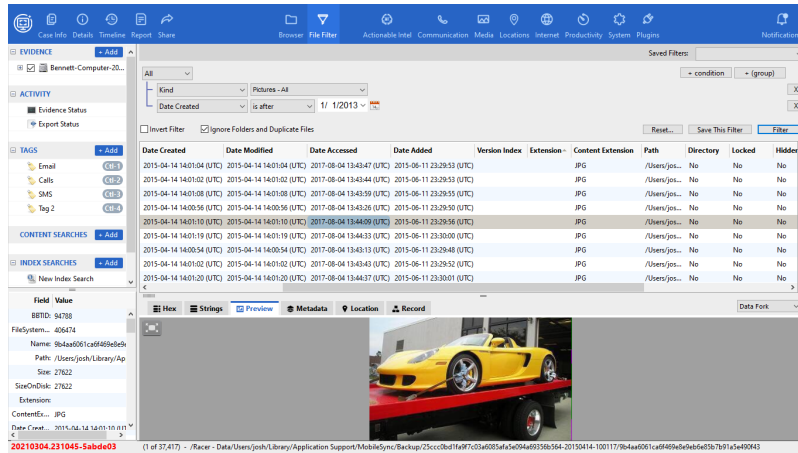
## File Filters

This chapter provides these topics about file filters in Inspector.

- [Individual File Filter Options](#)
- [Using File Filters](#)
- [Filtering within Specific Views](#)
- [Locating Live Victims](#)

The File Filter view and the Search features isolate information in a data set. The File Filter view isolates information by file attribute, such as file type and creation date. In contrast, the Content Search feature isolates information according to file content, such as alphanumeric keywords or regular expressions (RegEx). The Index Search feature isolates information based on information stored in the smart index.

File filtering is the quickest way to isolate data in a large data set.



Inspector has these built-in filter options.

| Filter               | Description                                                   |
|----------------------|---------------------------------------------------------------|
| List All Files       | Display all files on selected device                          |
| Name                 | Filter files by name                                          |
| Path                 | Filter files in a named directory (folder)                    |
| Kind                 | Filter by genus or category                                   |
| Extension            | Filter by file type based on extension (.doc, .txt, .jpg)     |
| Content Extension    | Filter by file type based on header information               |
| Extension Matching * | Filter by file type based on header and extension information |
| Tagged State         | Filter files that are tagged or not tagged                    |

| Filter                | Description                                                 |
|-----------------------|-------------------------------------------------------------|
| Tag Name              | Filter files by Tag Name                                    |
| Size                  | Filter by file size                                         |
| Owner                 | Filter by owner                                             |
| Group                 | Filter by group                                             |
| Permission            | Filter by permissions                                       |
| Date Created          | Filter by creation date                                     |
| Date Modified         | Filter by date modified                                     |
| Date Accessed         | Filter by last access date                                  |
| Date Added            | Filter by date added                                        |
| Inspector ID          | Filter by the record ID stored within the casefile database |
| File System ID        | Filter by the HFS catalog (node ID) / MFT ID number         |
| Hash Set              | Filter files with known hash values                         |
| Hash Set Category     | Filter files based on hash set category                     |
| File Hash             | Filter files based on a specific hash set                   |
| List Duplicate Files  | Filter the duplicate files by hash                          |
| File Entropy          | Filter by file entropy value                                |
| Soft Link Path        | Filter by soft link path                                    |
| Hard Link Target ID   | Filter by Hard Link Target ID used for Time Machine backups |
| Directory             | Filter by directory                                         |
| Locked                | Filter files with a locked flag                             |
| Resource Fork         | Filter files that have a resource fork                      |
| Alternate Data Stream | Filter files that have an alternate data stream             |
| Visibility            | Filter hidden or visible files                              |

| Filter                | Description                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------|
| iOS Hidden Item       | Filter iOS hidden items                                                                    |
| Metadata Field        | Filter on the metadata attribute field                                                     |
| Metadata Value        | Filter on the metadata attribute value                                                     |
| Metadata Field Value  | Filter simultaneously on metadata attribute field and value                                |
| Spotlight Field       | Filter on the spotlight attribute field                                                    |
| Spotlight Value       | Filter on the spotlight attribute value                                                    |
| Spotlight Field Value | Filter simultaneously on spotlight attribute field and value                               |
| Internal Filter       | Filter for displaying custom SQL from the details view                                     |
| Snapshot / VSC        | Filter files that have a Snapshot or Volume Shadow Copy version                            |
| OCR Image Text        | Filter by image files with text obtained by processing optical character recognition (OCR) |

\* A file extension is easily modified. A file header is more difficult to modify.

Each primary filter option in Inspector has additional modifiers that allow you to further refine filter results. For more information, see [Individual File Filter Options](#).

## Individual File Filter Options

You may use any of these file filter options on individual files within a case in Inspector.

- [List All Files](#)
- [Name](#)
- [Path](#)
- [Kind](#)
- [Extension](#)
- [Content Extension](#)
- [Extension Matching](#)
- [Tagged State](#)
- [Tag Name](#)
- [Size](#)
- [Owner](#)
- [Group](#)
- [Permission](#)
- [Dates Created, Modified, Accessed, and Added](#)
- [BL ID](#)
- [File System ID](#)
- [Hash Set](#)
- [Hash Set Category](#)
- [File Hash](#)
- [List Duplicate Files](#)
- [File Entropy](#)
- [Soft Link Path](#)
- [Hard Link Target ID](#)
- [Directory](#)
- [Locked](#)
- [Resource Fork](#)
- [Alternate Data Stream](#)
- [Visibility](#)
- [iOS Hidden Item](#)
- [Metadata Field](#)
- [Metadata Value](#)
- [Metadata Field Value](#)
- [Spotlight Field](#)
- [Spotlight Value](#)
- [Spotlight Field Value](#)
- [Internal Filter](#)
- [Snapshot \(APFS\) / Volume Shadow Copy \(NTFS\)](#)
- [OCR Image Text](#)

## List All Files

While the List All Files filter may take time to complete, it can be useful. For example, you can sort all files by ID, or by file type (content extension). The latter groups all known files together based on their file signature. During the sort process, a progress bar appears in the middle of the Case Manager window.

The File Filter displays up to 20 columns.

- Tagged State
- Evidence ID
- BL ID: The reference ID of a given file or folder within Inspector's casefile database
- FS ID: The filesystem ID parsed from the file record
- Name
- Size
- Logical size
- MD5
- Date Created
- Date Modified
- Date Accessed
- Date Added
- Version Index
- Extension: File extension stored in file system
- Content Extension: Displays the extension based on content header (file signature)
- Path
- Directory
- Locked: Displays locked/unlocked status (for example, read-only)
- Visible: Displays hidden/visible status
- Category
- SHA1
- SHA256
- Entropy

Right-click or press CTRL while you click anywhere in the Content pane. Click **Action > Save File Listing**. This saves the full file list of selected files. The time it takes depends upon the total number of files selected.

You can export file listings from the Content pane to a CSV or TSV delimited text file for importing into a spreadsheet or database application. For more information, see [Workspace Orientation](#).

## Name

The Name filter has five modifier options. You can simultaneously filter by more than one name by typing each name into the field to the right of the modifier field, separating each with a colon.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not



## Path

The Path filter has the same modifier options as the Name filter. However, you can filter only one path at a time.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

## Kind

The Kind filter may be the most commonly used filter in Inspector. It filters files based on a genus or category. Use this filter to locate similar files, such as picture or document files.

The Kind filter has 13 primary modifier options. Some of these primary modifiers have secondary modifier options.

- Application (Locates application types)

|     |                  |
|-----|------------------|
| All | All types below  |
| Mac | .app bundles     |
| Win | .exe executables |

- Archives (Locates these archive file types)

|           |                                                           |
|-----------|-----------------------------------------------------------|
| All       | All types below                                           |
| 7z        | 7-zip file (.7z)                                          |
| alz       | ALZip Archive file (.alz)                                 |
| bz2       | Burrows–Wheeler compressed file (.bz2)                    |
| cpio      | Unix CPIO Archive file (.cpio)                            |
| gz        | GNU compressed files (.gz)                                |
| jar       | Java Archive file (.jar)                                  |
| lzma      | Lempel-Ziv-Markov chain Algorithm compressed file (.lzma) |
| nsarchive | object's data stored to an archive file                   |
| pkg       | macOS installer package (.pkg)                            |
| rar       | Roshal Archive file (.rar)                                |
| sit       | Stuffit format files (.sit, .sitx, and .sea)              |
| tar       | Tape archive format (.tar)                                |
| uue       | Uuencoded file (.uue)                                     |
| wim       | Windows Imaging Format file (.wim)                        |
| xz        | XZ Compressed Archive (.xz)                               |
| zip       | PKWare based zip file (.zip)                              |

- Audio (Locates audio files)

- Databases (Locates these database file types)
 

|        |                                |
|--------|--------------------------------|
| All    | All types below                |
| db     | Database file (.db)            |
| sql    | SQL Database file (.sql)       |
| sqlite | SQLite Database file (.sqlite) |
- Disk Images (Locates these disk image file types)
 

|              |                                       |
|--------------|---------------------------------------|
| All          | All types below                       |
| aff4         | Advanced Forensic File Format (.aff4) |
| dmg          | Apple Disk Image (.dmg)               |
| img          | Macintosh Disk Image (.img)           |
| iso          | ISO-9660 standard image (.iso)        |
| sparsebundle | Apple Sparse Bundle (.sparsebundle)   |
| sparseimage  | Apple Sparse Image (.sparseimage)     |
- Emails (Locates these types of email)
 

|                      |                                |
|----------------------|--------------------------------|
| Apple Mail           | .eml, .emlx                    |
| Outlook 2011 for Mac | .olk14message, .olk14msgsource |
| Outlook 2016 for Mac | .olk15message, .olk15msgsource |
| Outlook for Windows  | .ost, .pst                     |
- Folder (Locates all folders and directories)
- iWork (Locates these iWork Office file types)
 

|         |                                             |
|---------|---------------------------------------------|
| All     | All types below                             |
| Keynote | iWork Keynote (presentation) files (.key)   |
| Numbers | iWork Number (spreadsheet) files (.numbers) |
| Pages   | iWork Pages (word processor) files (.pages) |
- Office Documents (Locates these Microsoft Office file types)
 

|            |                                          |
|------------|------------------------------------------|
| All        | All types below                          |
| Excel      | Microsoft Excel files (.xls, .xlsx)      |
| PowerPoint | Microsoft PowerPoint files (.ppt, .pptx) |
| Word       | Microsoft Word files (.doc, docx)        |
- PDF (Locates all .pdf files)
- Pictures (Locates these picture file types)
 

|      |                                                                   |
|------|-------------------------------------------------------------------|
| All  | All types below                                                   |
| BMP  | bitmap raster graphics image file format (.bmp)                   |
| GIF  | Graphics Interchange Format (.gif)                                |
| HEIC | High Efficiency Image File Format (.HEIC)                         |
| JPG  | Joint Photographic Experts Group format (.jpg, .jp2, .jpeg)       |
| KDC  | Bitmap image formate used by several Kodak digital cameras (.kdc) |
| PNG  | Portable Network Graphics (.png)                                  |
| PSD  | Adobe Photoshop (.psd)                                            |
| TIFF | Tagged Image File Format (.tif, .tiff, .tif/tiff)                 |
| XBM  | X BitMap, a plain text binary image format (.xbm)                 |

- Plists (Locates .plist file types)
- Videos (Locates these video file types)
  - Multimedia container format defined by the Third Generation Partnership Project (.3gp, .3g2)
  - Audio Video Interleave (.avi)
  - Digital video file (.dv)
  - Flash Video (.flv)
  - Digital multimedia container format (.m4v, .mp4)
  - Quicktime file format (.mov)
  - Standard for lossy compression of video and audio (.mpeg, .mpg)
  - Video Object is the container format in DVD-Video media (.vob)
  - Windows Media Video (.wmv)
  - Low resolution GoPRO video files (.lrv)

## Extension

The Extension filter has five modifier options. You can simultaneously filter by more than one file extension by typing each file extension into the field to the right of the modifier field, separating each with a colon.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

File extensions are assigned to a file by an application or a user. On Mac computers, files may not have extensions, or the file extensions may not be visible.

## Content Extension

The Content Extension filter has the same modifier options as the Extension filter. Filtering by Content Extension is based on file signature, rather than on the visible extension within the file name. You can simultaneously filter by more than one content extension by typing each into the field to the right of the modifier field, separating each with a colon.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

## Extension Matching

The Extension Matching filter compares file extensions to file signatures. Use this filter to isolate files with extensions and signatures that match or don't match. (A user can easily modify a file extension, but a file signature is more difficult to modify.)

The Extension Matching filter has two modifier options.

- Extensions Don't Match (default)
- Extensions Match

## Tagged State

The Tagged State filter has three modifier options.

- Tagged Files (default)
- Untagged Files
- Both Tagged and Untagged Files

## Tag Name

The Tag Name filter has five modifier options.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

## Size

The Size filter has primary and secondary modifier options. Both modifiers must be set for the filter to function. After modifiers are set, click **Filter**.

First, choose from this list of modifiers.

- equals
- is less than
- is greater than (default)
- is not
- is <= to
- is >= to

Next, type a custom file size in the text field and choose a unit of measure.

- Bytes
- KB (Kilobytes) (default)
- MB (Megabytes)
- GB (Gigabytes)

## Owner

The Owner filter has six modifier options.

- equals
- is less than
- is greater than (default)
- is not
- is <= to
- is >= to

## Group

The Group filter has six modifier options.

- equals
- is less than
- is greater than (default)
- is not
- is <= to
- is >= to

## Permission

The Permission filter has six modifier options.

- equals
- is less than
- is greater than (default)
- is not
- is <= to
- is >= to

## Dates Created, Modified, Accessed, and Added

The Date Created, Date Modified, Date Accessed, and Date Added filters have five modifier options.

- is between (default)
- is before
- is after
- is exactly
- is not

To the right of the date field, click the calendar icon. On the calendar, click < or > to scroll through the months. Or, at the top of the calendar, choose a month and year from the drop-down menus. Select a number to choose a day of the month. The date text field is populated, and the calendar closes.

To modify the date manually, in the date field click to select a month, day, or year value, and type the desired numeric value into the text field. To modify the date incrementally, in the date field click to select a month, day, or year value. To the right of the date field, click the up or down arrows to increase or decrease the date value incrementally.

## BL ID

The BL ID is a unique internal file identifier. It is different from the file system ID number. The Inspector ID number is generated during ingestion for every file. This is done because some files do not have a file ID (deleted files, files from archives, ingested file or folder items). Inspector uses this as an internal tracking system. They are only unique for the case file in which they reside. The filter option has six modifier options.

- equals
- is less than
- is greater than (default)
- is not
- is <= to
- is >= to

## File System ID

The File System ID filter option has six modifier options.

- equals
- is less than
- is greater than (default)
- is not
- is <= to
- is >= to

Folders and files on a volume formatted in HFS or HFS+ are assigned a unique Catalog Node ID (CNID). Using the File System ID file filter, you can search for folders and files by a specific Catalog Node ID, or within a Catalog Node ID numerical range. NTFS files will use the MFT ID.

**Note:** The order folders and files were created on an HFS volume can be determined from the CNID; once assigned to a file/folder, the CNID remains the same and subsequently created folders and files continue to receive new, unique, and sequentially increasing CNID numbers.

## Hash Set

The Hash Set filter supports positive and negative hash value filtering against one or more hash sets. For more information, see [Hash Set and File Signature DB Management](#). This filter has two modifier options.

- Files in Hash Set (default)
- Files Not in Hash Set

You can download hash sets from Cellebrite. Inspector can use those hash sets and import EnCase (6.19 and lower), NSRL (full), and text-based (one hash value per line, with each line separated by a carriage return) hash sets. Additionally, you can create custom hash sets from file hash values generated during a case examination.

The Hash Set filter is available only after you run the Known Files processor on a device in the case, using one or more hash sets (bundled and custom). Each hash set you select before running the Known Files processor is available as a Hash Set filter option.

To create a positive hash filter, which isolates only files with hash values matching those in the chosen hash set, choose the Files in Hash Set option and select a bundled or custom hash set. To create a negative hash filter, which isolates only files with hash values not matching those in the chosen hash set, choose the File Not in Hash Set option and select a bundled or custom hash set.

## Hash Set Category

The Hash Set Category filter allows for numeric filtering of file hash categories (for hash sets with categories, such as PhotoDNA, S21). Hash sets in Inspector can be assigned a number from 0 through 9. The filter has six modifier options.

- equals
- is less than
- is greater than (default)
- is not
- is <= to
- is >= to

**Note:** Hash set categories have different meanings depending on the hash set being used. To provide flexibility to all users, Inspector shows only the Hash Set Category number.

## File Hash

The File Hash filter has five modifier options.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

You can filter by hash values using all characters of a hash value or by using only part of a hash value. You can filter data based on any of these hash values (MD5, SHA-1, or SHA-256). This filter only works after you run the Hashes processor on a device in the case.

## List Duplicate Files

The List Duplicate Files filter option has no modifiers. It shows all duplicate files based on hash value. This filter only works after you runs the Hashes processor on a device in the case.

## File Entropy

The File Entropy filter has three modifier options.

- High (>0.8)
- Medium (0.5 - 0.8)
- Low (<0.5)



## Soft Link Path

You can use this filter to find soft links (symbolic links) created in macOS. The Soft Link Path filter has six modifier options.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

## Hard Link Target ID

You can use this filter to find files within a Time Machine backup. The Hard Link Target ID filter has six modifier options.

- equals
- is less than
- is greater than (default)
- is not
- is <= to
- is >= to

## Directory

The Directory filter has three modifier options.

- Directories only
- Files only
- both directories and files (default)

## Locked

The Locked filter has three modifier options.

- Locked files only
- Unlocked files only
- both Locked and Unlocked files (default)

Locked files are write-protected (read-only). A standard user can open these files and perhaps copy them to a different location. However, a locked file cannot (under normal circumstances) be modified, renamed, or deleted.

## Resource Fork

The Resource Fork filter has three modifier options.

- only files with a Resource Fork
- only files without a Resource Fork
- files with or without a Resource Fork (default)

In macOS, “design element” information is stored in a file’s resource fork. “Raw” information, such as text, is stored in a file’s data fork.

## Alternate Data Stream

The Alternate Data Stream filter has three modifier options.

- only files with an Alternate Data Stream
- only files without an Alternate Data Stream
- files with or without an Alternate Data Stream (default)

## Visibility

The Visibility filter has three modifier options.

- Visible files only
- Invisible files only
- both Visible and Invisible files (default)

Many system files are hidden in macOS to prevent accidental user modifications. However, users can manually hide both folders and files by highlighting the folder or file name and typing a dot [.] at the beginning of the name. The Visibility filter does not include files and folders hidden by users in filter results. To include files and folders hidden by users in results, also use the Name filter modified by starts with . (dot).

## iOS Hidden Item

The iOS Hidden Item filter has no modifiers. It shows iOS Hidden Items.

## Metadata Field

A Metadata Field is based on the metadata Field column seen in the File Information pane. For example, a metadata field could be Megapixels, Aspect Ratio, or Skin Tone. Not all files contain the same types of metadata. This filter isolates only files containing metadata you specify in the metadata field.

The Metadata Field filter option has five modifier options.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

You can simultaneously filter by more than one metadata item by typing each metadata item into the field to the right of the modifier option field, separating each item with a colon.

## Metadata Value

The Metadata Value filter has five modifier options.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

You can simultaneously filter by more than one metadata value by typing each value into the text field to the right of the modifier option field, separating each item with a colon.

Some metadata items, such as picture aspect ratios, contain a colon in the item name (for example, a 4:3 aspect ratio). In this case, the colon symbol must be "escaped" to prevent the filter from giving results with "4" and "3" in the metadata. To filter files by metadata values that have a colon, add an additional colon. For example, to filter for the aspect ratio 4:3, type **4::3** into the filter criteria field.

## Metadata Field Value

The filter combines the Metadata Field filter with the Metadata Value filter. The modifier options listed for the Metadata Field and the Metadata Value filters are present in this combined filter.

## Spotlight Field

To use this filter, the Spotlight Index must be parsed in Advanced processing options. The Spotlight Field filter option has five modifier options.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

## Spotlight Value

To use this filter, the Spotlight Index must be parsed in Advanced processing options. The Spotlight Value filter option has five modifier options.

- contains (default)
- does not contain
- starts with
- ends with
- is
- is not

## Spotlight Field Value

This filter combines the Spotlight Field filter with the Spotlight Value filter. The modifier options listed for the Spotlight Field and the Spotlight Value filters are present in this combined filter.

## Internal Filter

You can select this filter when the File Filter view shows a custom SQL value from the Details view (for example, when double-clicking on a bar graph element in the Details - Artifacts view). This allows for the data to be sorted, refreshed, and further filtered. If you attempt to select the Internal Filter option when building a custom filter, Inspector automatically switches to the List All Files filter instead.

## Snapshot (APFS) / Volume Shadow Copy (NTFS)

The Snapshot filter works on macOS computers which have the APFS file system. Volume Shadow copies exist on Windows NTFS filesystems. The Snapshot/Volume Shadow Copy filter option has four modifier options.

- only files with changes in a Snapshot/VSC
- only files that exist in more than one Snapshot/VSC (Active partition included)
- only files that are unique to the Active partition or to a Snapshot/VSC
- all files

In either the File Filter view or the Browser view, double-click any file that is—or has—a Volume Shadow Copy version, and a separate File History window appears. In this window, all Volume Shadow Copy versions of a file can be further analyzed.

**Important:** Hashing must be run on not only the active partitions but also the Snapshots or VSCs in order for these filters to work.

## OCR Image Text

Optical character recognition (OCR) converts text detected in the image into plain text which can be indexed and then searched. This process is limited to these image types.

- pdf
- tiff
- bmp
- png
- jpg
- gif

This filter has these options.

- Only files with OCR Image Text
- Only files without OCR Image Text
- Files with or without OCR Image Text

Text obtained through OCR appears on the Strings tab in the File Content view after this label:

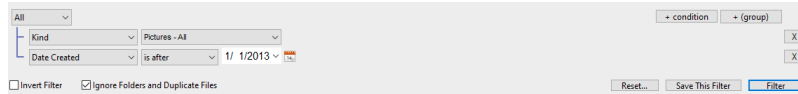
\*\*\*\*\* OCR Image Text \*\*\*\*\*

You can search OCR text with an index search, but not with a content search, as OCR text does not exist as plain text.

## Using File Filters

In the Component list under Evidence, select a device. On the toolbar, click **File Filter**. Click **+ Condition** or **+ Group** to add a filter criteria row or group.

This example shows a file filter to isolate all picture file types created after January 1, 2013.



Add the **Kind** condition and the modifier **Pictures - All**. Next, add the **Date Created** condition and the modifier **is after**, then set the date to **1/1/2013**. Click **Filter**. The results show all .bmp, .gif, .heic, .jpg, .kdc, .png, .psd, .tiff, and .xbm picture file types, further isolated to files created after January 1, 2013.

To suppress folders and file duplicates in the results, mark the **Ignore Folders and Duplicate Files** checkbox. To filter files that match the inverse of the filter criteria, mark the **Invert Filter** checkbox.

To remove a filter criteria row or group, click **X**.

## Saving and Managing File Filters

To save a file filter for later use, click **Save This Filter**. Type a name for the filter and click **OK**. Inspector saves the current filter settings. Saved filters appear in the **Saved Filters** list in the top right corner of the Content pane.

Saved file filters also appear in the Inspector Search view and may be applied to further refine search results. For more information, see [Search](#).

To rename or remove a saved filter, in the top right corner of the Content pane click **Saved Filters > Manage Saved Filters**. The User Created Filters window appears.

- To rename a filter, select the filter from the list, and then click **Rename**. Type a new filter name and click anywhere in the window to escape the text field.
- To remove a saved file filter, select the filter from the list, and then click **Remove**.

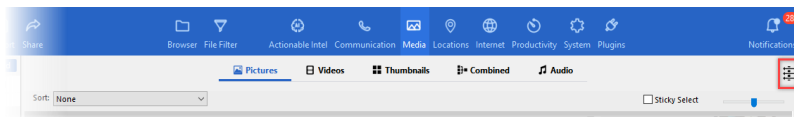
## Applying a Preset Filter or Saved File Filter

To apply a preset filter or a saved filter, in the **Saved Filters** list, select the filter and then click **Filter**.

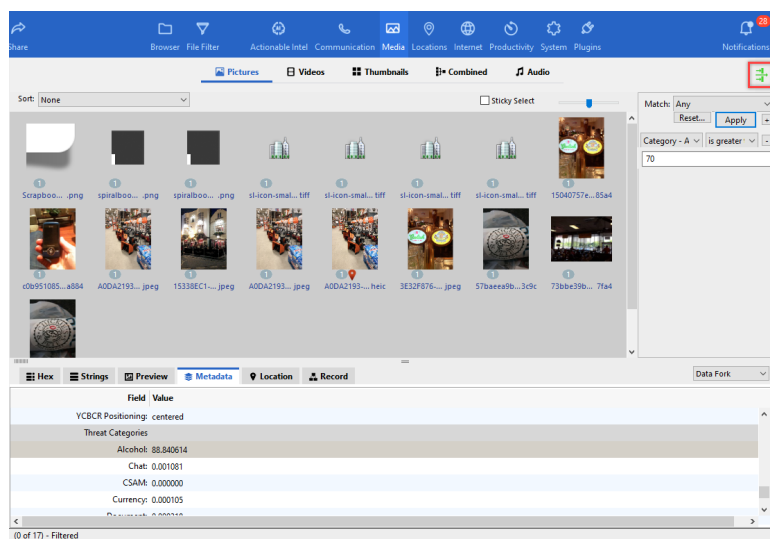
To clear and reset the current filter settings, click **Reset**.

## Filtering within Specific Views

Several views in Inspector include a file filter. The filter options that are available depend upon which view is in use.



The button changes in appearance such that the arrows are reversed, and a filter pane appears in the right portion of the Content pane. When a filter is applied, the Show/Hide Filter button is green.



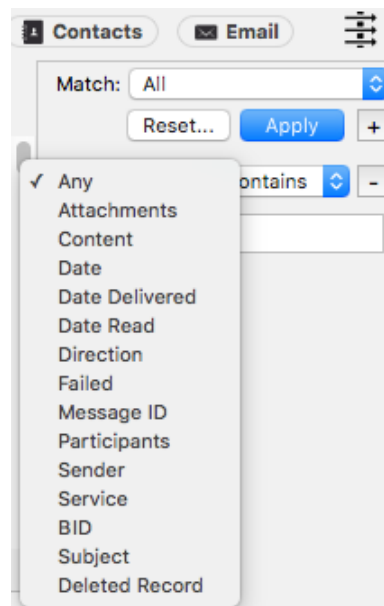
To show or hide the file filter, toggle **Show/Hide Filter** (three arrows) at the top right of the Content pane.

When Show/Hide Filter is black, no filter is applied. While at least one filter is applied, it is green.

To create a filter for a view, to the right of Apply, click **+** (**add**). In the filter field, the default is Any. Choose an appropriate filter option and set the modifiers. Repeat this process to add more filter options.

To remove a filter option, to the right of the filter, click **-** (**remove**). To remove all filters and return to showing all files, click **-** (**remove**) for each filter, then click **Apply**.

This example shows filter options for the Messages sub-view of the Communications view.



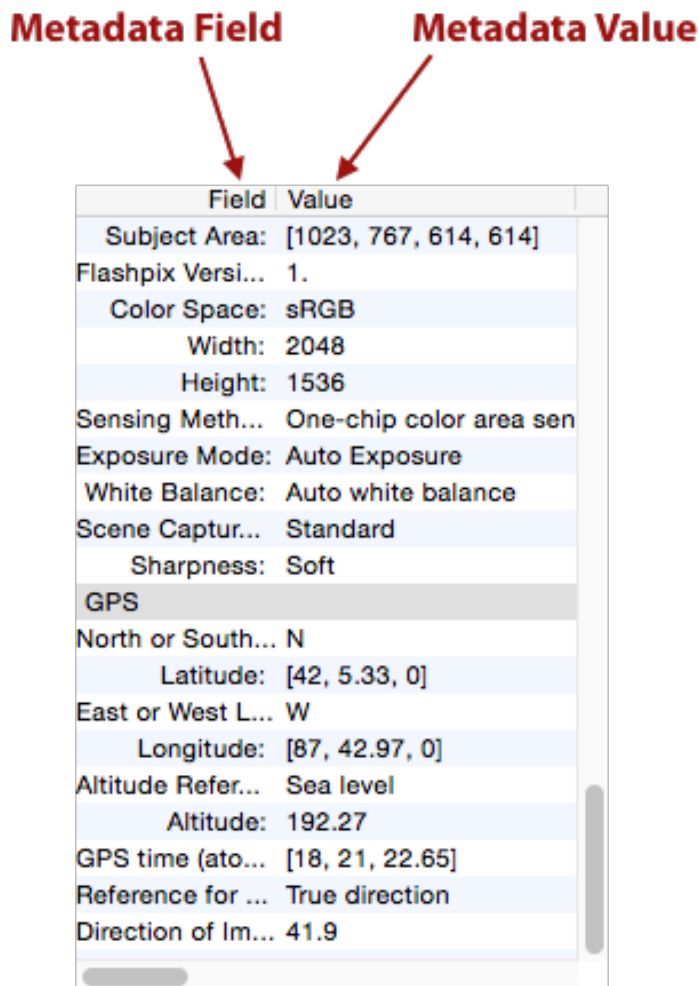
## Locating Live Victims

Using the Inspector Locations and File Filter or Media File Filter features together, an investigator may quickly isolate picture and/or video files containing geolocation metadata with just a few keystrokes. The investigator may then locate additional picture and video files taken at the same location and/or with the same iPhone, iPad, or other camera make and model by applying a filter containing specific longitude and latitude coordinates, or the smart device or camera model name.

The Inspector Metadata Field filter isolates files containing specified metadata attributes (seen in the above screenshot, left column). For example, choose the Metadata Field file filter to ask Inspector to 'show me all the files containing GPS, latitude, longitude, and EXIF metadata.' Inspector also has a built-in filter, Geo Location, to locate data containing Geolocation information based on the presence of geolocation Metadata Fields.

The Metadata Value filter isolates files containing specified metadata values (seen in the above screenshot, right column) such as an actual longitude or latitude coordinate or a specific camera make. For example, choose the Metadata Value file filter to ask Inspector to 'show me all the files containing the latitude coordinate [43, 38, 33.21].'

In this example, we combine a geolocation filter in the Media view, and the Metadata Value file filter to locate pictures taken at the same location.



The screenshot shows a table with two columns: 'Field' and 'Value'. Red arrows point from the labels 'Metadata Field' and 'Metadata Value' to the respective column headers. The table contains various metadata entries, including EXIF data and GPS coordinates.

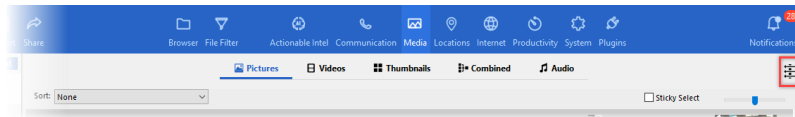
| Field              | Value                   |
|--------------------|-------------------------|
| Subject Area:      | [1023, 767, 614, 614]   |
| Flashpix Versi...  | 1.                      |
| Color Space:       | sRGB                    |
| Width:             | 2048                    |
| Height:            | 1536                    |
| Sensing Meth...    | One-chip color area sen |
| Exposure Mode:     | Auto Exposure           |
| White Balance:     | Auto white balance      |
| Scene Captur...    | Standard                |
| Sharpness:         | Soft                    |
| <b>GPS</b>         |                         |
| North or South...  | N                       |
| Latitude:          | [42, 5.33, 0]           |
| East or West L...  | W                       |
| Longitude:         | [87, 42.97, 0]          |
| Altitude Refer...  | Sea level               |
| Altitude:          | 192.27                  |
| GPS time (ato...   | [18, 21, 22.65]         |
| Reference for ...  | True direction          |
| Direction of Im... | 41.9                    |



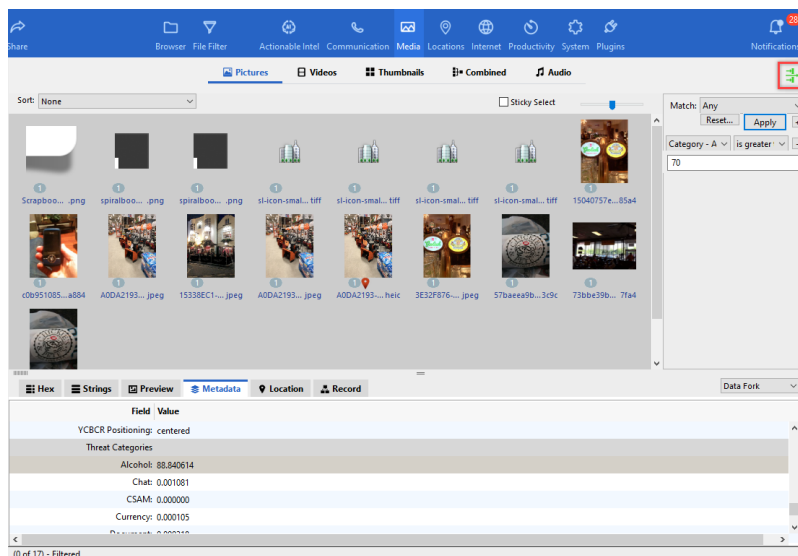
## Locating Picture or Video Files Created at the Same Location

To isolate media files containing geolocation metadata, in the Component list under Evidence select a device. On the toolbar, click **Media**.

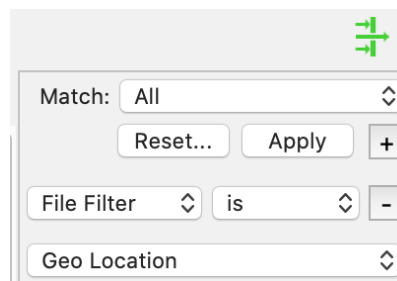
To isolate media files containing geolocation metadata, click **Show/Hide Filter** (three arrows) below the right side of the toolbar.



The button changes in appearance such that the arrows are reversed, and a filter pane appears in the right portion of the Content pane. When a filter is applied, the Show/Hide Filter button is green.



To the right of Apply, click **+ (add)**. The default filter is File Filter | is | Current File Filter. Click **Current File Filter** and select **Geo Location**.



Click **Apply** to see only media files containing geolocation metadata.

| Field              | Value                  |
|--------------------|------------------------|
| White Balance:     | Auto white balance     |
| 35mm Focal L...    | 33                     |
| Scene Captur...    | Standard               |
| Unknown Tagl...    | [4.12, 4.12, 2.4, 2.4] |
| Unknown Tagl...    | Apple                  |
| Unknown Tagl...    | iPhone 5 back camera   |
| GPS                |                        |
| North or South...  | N                      |
| Latitude:          | [43, 38, 33.21]        |
| East or West L...  | W                      |
| Longitude:         | [79, 23, 6.78]         |
| Altitude Refer...  | Sea level              |
| Altitude:          | 94.8                   |
| GPS time (ato...   | [17, 57, 41]           |
| Reference for ...  | True direction         |
| Direction of Im... | 329.16                 |
| GPS Date:          | 2014:02:15             |

To find media files containing the same GPS coordinates, in the Content pane select a file that has GPS metadata. In the bottom left corner of the Case Window in the File Information pane, GPS metadata values for the selected file appear in the GPS section in the Value column. Make note of the GPS longitude or latitude value. In this example, we use latitude [43, 38, 33.21].

On the toolbar, click **File Filter**. The File Filter view appears.

At the top of the Content pane, select the existing file filter drop-down menu and select **Metadata Value**.

A secondary drop-down menu and text field appears. Leave the default (contains) selected and in the text field, type the previously noted longitude or latitude coordinates:

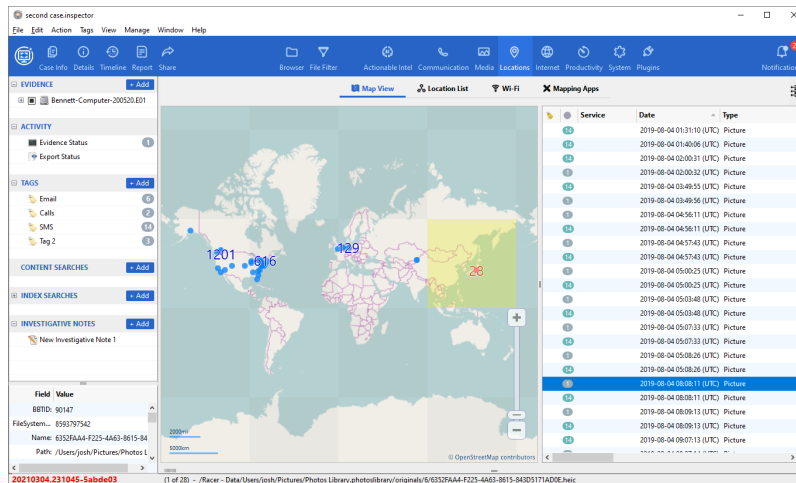
Click **Filter**, and Inspector isolates files containing the defined longitude or latitude coordinates. On the toolbar, click **Media** to switch back to the Media view. To the right of the Apply button, click **+** (add). Inspector configures a second File Filter | is | Current File Filter by default. Leave this setting as is and click **Apply**.

Inspector applies the Metadata Value filter and displays only the pictures containing latitude [43, 38, 33.21] metadata.

Mac and iPhone forensic analysts may use the same file filtering technique to isolate files taken by an iPhone (or any other camera type). To do so, on the toolbar click **File Filter** and select the **Metadata Value** filter. In the text field, type iPhone and click **Filter**. On the toolbar, click **Media** to switch back to the Media view. Click **Apply**. Inspector shows the pictures containing an iPhone metadata value.

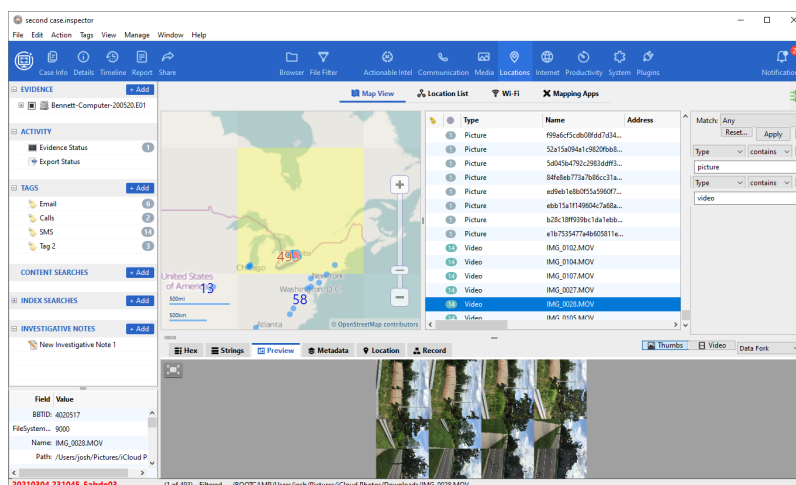
A second method for locating picture or video files created at the same location is to use the Map View sub-view in the Locations view. On the toolbar, click **Locations**. With the Map View sub-view selected, the Content pane displays a map on which data containing geolocation information is plotted.

The map is divided into square regions. When you click a region, it is highlighted in yellow. Data from information in that square of the map is listed in the right section of the Content pane.



The Type column reveals the type of data the geolocation was extracted from. Depending on the device, location data may be stored in various applications and system files. Pictures and Videos contain location data are listed with the type Picture and Video.

Using the zoom slide-bar, you can focus on specific geographic location. After zooming in on the area of interest, apply a filter to display only picture and video files. Double-click on the **Latitude** column to sort the pictures and videos by location. Picture and videos taken at the same location are grouped together. When a file is selected in the Content pane, the associated data point on the map is changed from blue to pink. The File Content view can be used to preview the file.



Map View provides an interactive interface to locate and review pictures and videos of interest taken at a location of interest. For more information, see [Locations, Internet, and Productivity Views](#).

## Sorting Media Files by Calculated Skin Percentage

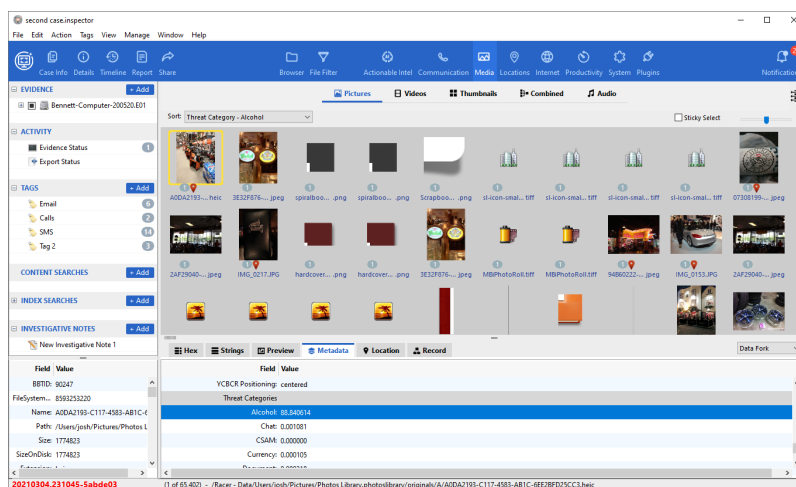
To sort filtered media files so that files with the highest calculated skin percentage appear first, on the toolbar click **Media**.

In the top left corner of the Content pane, select the secondary drop-down menu and choose **Calculated Skin %**.

Inspector sorts the media files, and the media file containing the highest calculated skin percentage appears first. This feature is quite useful if there are many media files created at the same location.

## Sorting Media Files by Image Analyzer Categories

When media files are categorized by Threat Category, they can be sorted and filtered by threat category. To sort media files so that files with the highest calculated Threat Category value appear first, on the toolbar click **Media**.



In the **Sort** field, choose one of these threat categories.

- Threat Category – Alcohol
- Threat Category – Chat
- Threat Category – CSAM
- Threat Category – Currency
- Threat Category – Documents
- Threat Category – Drugs
- Threat Category – Extremism
- Threat Category – Gambling
- Threat Category – Gore
- Threat Category – ID/Credit Cards
- Threat Category – Porn
- Threat Category – Swim/Underwear
- Threat Category – Vehicles
- Threat Category – Weapons

Inspector sorts the media files, and the media file containing the highest calculated percentage in the selected Threat Category appears first. This feature is quite useful if there are many media files created at the same location. Image Analyzer threat categories may be more accurate than skin percentage.

## Mapping GPS Metadata Using Google Maps

To map geolocation metadata, select a file, and at the top of the File Content view, click **Location**. If the analysis workstation is a non-networked machine, a Mercator map with red crosshairs representing the file's approximate longitude and latitude coordinates displays along with several of the file's actual geolocation metadata attributes and values (i.e., latitude, longitude, timestamp, etc.).

If the analysis workstation has an Internet connection, click **Show on Google Maps**. A default browser window opens and displays (potentially) an address, a street view picture, and a satellite view based on the file's GPS metadata.

## Mapping GPS Metadata Using Google Earth

Files containing GPS information can be selected, exported to a .kmz or .kml file, and mapped with the Google Earth application.

1. Select file(s) containing GPS data, click **Action > Export Selected Location Data As**, and then choose either KMZ or KML format.
2. In the Export dialog box, type a file name and choose or create a destination folder, and then click **Export**.

Inspector exports the GPS data to a .kmz or .kml file in the destination folder.

3. Open the .kmz or .kml file in Google Earth.  
Google Earth displays a pushpin for each file. Each pushpin is also listed in the Google Earth sidebar Places section.

We have now located media files that contain geolocation data, isolated the files containing the same GPS coordinates, sorted those results by calculated skin tone percentage, and mapped the results.

Remember that media created using any camera with enabled GPS tracking features, such as the iPhone and iPad Location Services feature, may contain geolocation metadata. Forensic analysts may find geolocation artifacts on a Mac computer if the user attached the camera or smart device to the computer.

## Search

There are two types of Searches. The Content Search feature isolates information according to file content such as alphanumeric keywords or regular expressions. The Index Search feature isolates information by querying information stored in the Smart Index. Any fields or documents that have been indexed can be used to find information of interest. Keep in mind unallocated space is not indexed. To find information in unallocated space, a Content Search must be used.

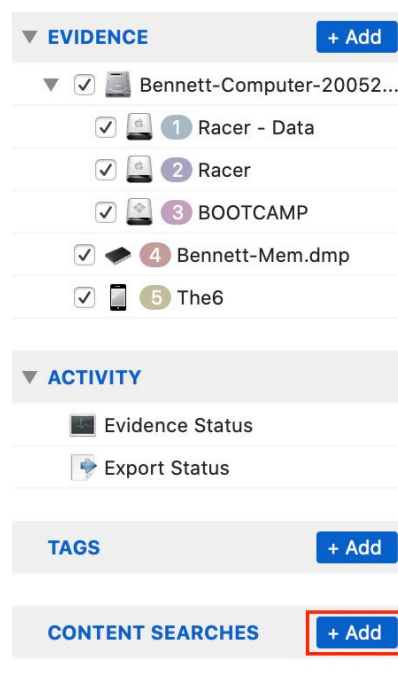
File Filtering can be used in conjunction with Content Searches to further isolate information.

This chapter provides these topics about searching in Inspector.

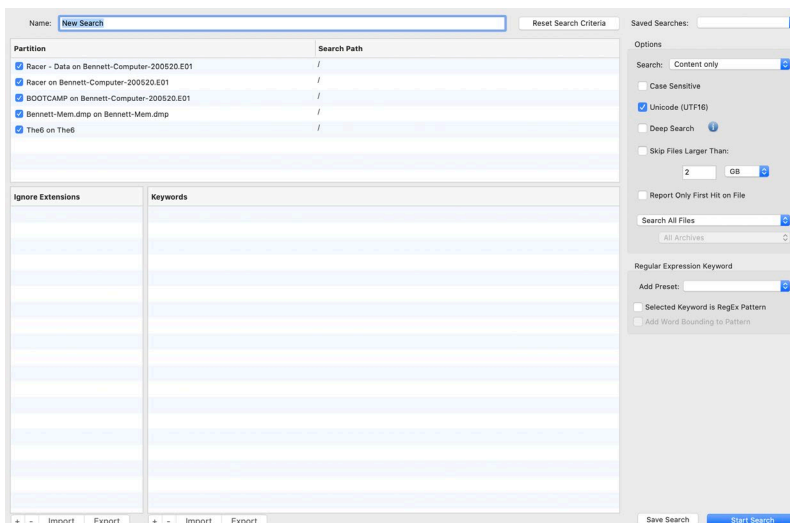
- [Content Keyword Searches](#)
- [Saved Content Search Settings](#)
- [Applying Filters to a Content Search](#)
- [Viewing Content Search Results and Criteria](#)
- [Index Searching](#)
- [Bulk Extraction Searches on Memory Files](#)

## Content Keyword Searches

To execute a content search, click **Add** next to Content Searches in the Component list.



Inspector names each new search "New Search #" (appended with an incremental number) automatically. To avoid confusion, always add a unique and descriptive search name at the top of the Content pane in the **Name** field when defining new search criteria.

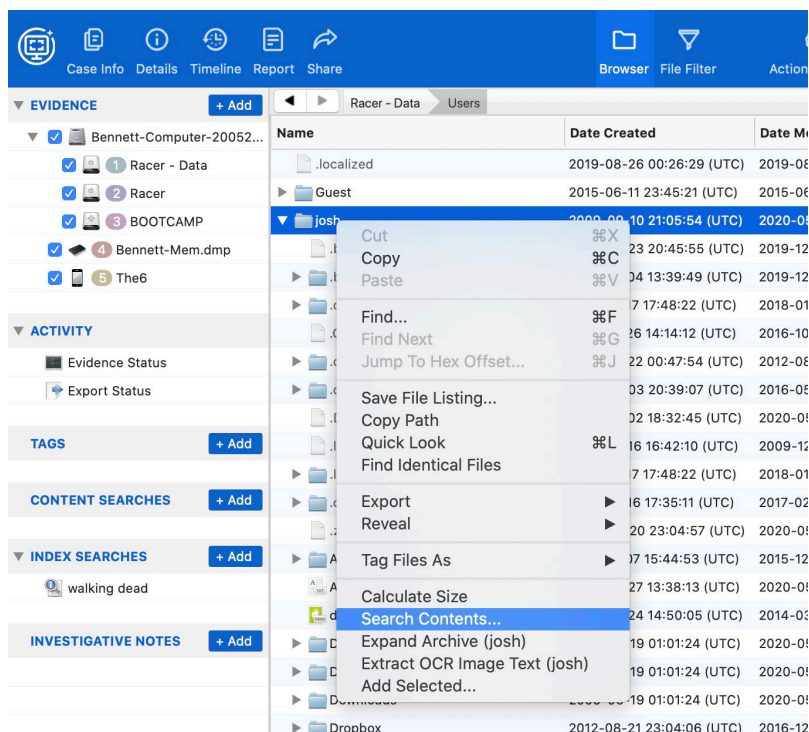


Once a content search is created, it is shown in the Component list under Content Searches. Double-click a saved search name to rename it at any time during the examination.

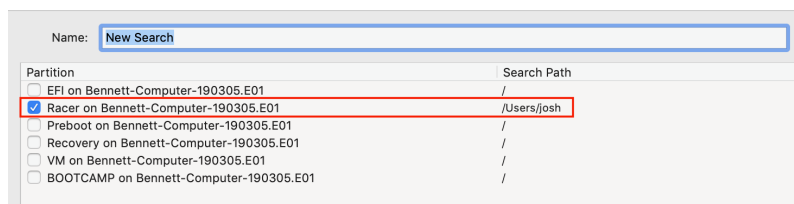
Content searches can be refined to search specified areas of the media. Searches can be directed to specific volumes by selecting the volume where it is listed in the Content pane. By default, content searches are set to search from the root directory of the volume.

To confine a search to a specific directory, type or paste the path in the **Search Path** field. To copy-paste a path name, navigate to the device in the Browser view. In the Content pane, right-click or CTRL+click on a folder and choose **Copy Path**. Click **Add** next to Content Searches in the Component list. In the Content pane to the right of the selected device name (under the Partition column), double-click the **Search Path** field and press CMD+V or CTRL+V. To the left of the selected device name (under the Partition column), mark the checkbox. Inspector searches the selected folder.

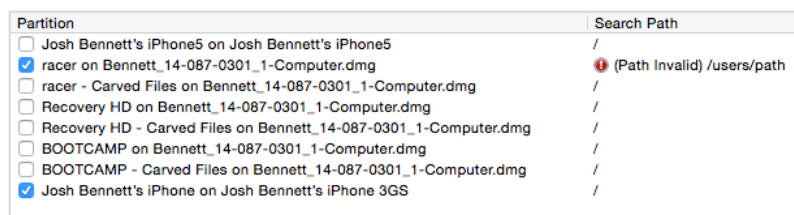
A secondary method for choosing the areas to search is to use **Search Contents** from the contextual menu. This can be done while from the Browser view. While in the Content pane, right-click or CTRL+click on a folder and choose **Search Contents** from the context menu.



A new search window opens with the appropriate partition and search path checkbox selected.



To search the entire device, leave the Search Path field as it appears with just /. If a path name is incorrectly entered into a Search Path field or if the typed path does not exist in the file system, a red error badge (!) appears next to the field. Once a valid path name is correctly entered, the error disappears.





## Adding Keywords to Content Searches

In the Content pane at the bottom of the Keywords section, click **+** (**add**) and enter a keyword. Optionally, in the Content pane in the Regular Expressions section, select the **Selected Keyword is RegEx Pattern** checkbox to save the keyword as a regular expression. For example, to add the search term “slim jim” and search for keyword occurrences with either a space or no space between “slim” and “jim”, add the keyword `slim\s{0,1}jim`.

Mark the **Selected Keyword is RegEx Pattern** checkbox. The new keyword is added as a search term and added to the **Add Preset** drop-down menu as a regular expression preset.

To add an existing text file containing a list of keyword search terms to a search, at the bottom of the Keywords section, click **Import**. The file for import must be UTF-8 encoded, as other encodings may not import correctly. Click **Export** to save the current keyword search term list to a text file for later use. To remove a keyword or keywords from the Keywords list, select a keyword or multiple keywords, and click **- (remove)**.

Inspector ignores files with a given extension when these extensions are added to the Ignore Extensions list. Items are added to the Ignore Extensions list in the same way they are added to the Keywords list.

## Regular Expression Presets

Inspector includes several regular expression presets. Select these presets in the Regular Expressions section with the **Add Preset** menu. You can also edit regular expressions after selecting them.

| Preset Option                | Regular Expression                                                                                                                                                                 |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Social Security Number       | <code>^([?!000])(?!666)([0-6\d{2}]7[0-2][0-9] 73[0-3] 7[5-6][0-9] 77[0-1]))-([?!00]\d{2})-([?!0000]\d{4})\$</code>                                                                 |
| UK National Insurance Number | <code>^[A-CEGHJ-PR-TW-Z]{1}[A-CEGHJ-NPR-TW-Z]{1}[0-9]{6}[A-DFM]{0,1}\$</code>                                                                                                      |
| MAC Address                  | <code>((\d ([a-f] [A-F])){2}:){5}(\d ([a-f] [A-F])){2}</code>                                                                                                                      |
| IP Address                   | <code>\b(25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\. (25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\. (25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\. (25[0-5] 2[0-4][0-9] [01]?[0-9][0-9]?)\b</code> |
| Email Address                | <code>[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}</code>                                                                                                                       |

| Preset Option              | Regular Expression                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Email Address (Simple)     | <code>[A-Z0-9-_.+%]{1,64}@([A-Z0-9-]{1,63}\.([A-Z]{2,63} ((XN)--[A-Z0-9]{1,59})))</code>                                                                                                                                                                                                                                                                                |
| URL                        | <code>(([htf]tp[s?]:\V) www\.[^\[\]\(\)\n\r\t+] (((012)?[0-9]{1,2}\.){3}(012)?[0-9]{1,2})V ([^\[\]\(\),;'\&amp;lt;&amp;gt;\n\r\t+] ([^\[\]\(\),;'\&amp;lt;&amp;gt;\n\r\t) (((012)?[0-9]{1,2}\.){3}(012)?[0-9]{1,2}))</code>                                                                                                                                             |
| International Phone Number | <code>^\+[1-9][0-9]*([([0-9]*) -([0-9]*)-)?[0]?[1-9][0-9\ -]*\$</code>                                                                                                                                                                                                                                                                                                  |
| Valid US Phone Number      | <code>^(((\d{3})\d{3})(  -\.)) (\d{3})\d{3}))?\d{3}(   -\.)?\d{4}((  -\.)?([Ee]xt [Xx])[. ]?(  -\.)?\d{4})?\$</code>                                                                                                                                                                                                                                                    |
| UK Phone Number            | <code>((\+44)? ?(\0\)? ?) (\0)( ?[0-9]{3,4}){3}</code>                                                                                                                                                                                                                                                                                                                  |
| Valid UK PostCode          | <code>((^[BEGLMNS][1-9]\d?)(^W[2-9])(^[A[BL] B[ABDHLNRST] C[ABFHMORTW] D[ADEGHLNTY] E[HNX] F[KY] G[LUY] H[ADGPRSUX] I[GMPV] J[E] K[ATWY] L[ADELNSU] M[EKL] N[EGNPRW] O[LX] P[AEHLOR] R[GHM] S[AEGKL-PRSTWY] T[ADFNQRSW] UB W[ADFNRSV] YO ZE)\d\d?)(^W1[A-HJKSTUW0-9]) ((^WC[1-2]) ^EC[1-4]) ^SW1)[ABEHMNPRVWXY])(\s*)?([0-9][ABD-HJLNP-UW-Z]{2}))\$ ^GIR\s?0AA\$</code> |
| US PostCode                | <code>((\d{5}-\d{4}) \d{5})</code>                                                                                                                                                                                                                                                                                                                                      |
| Canada PostCode            | <code>((?i)[ABCEGHJKLMNPRSTVXY]\d[ABCEGHJKLMNPRSTVWXYZ]\s?\d[ABCEGHJKLMNPRSTVWXYZ]\d)</code>                                                                                                                                                                                                                                                                            |
| Date                       | <code>^((((0?[13578]) (1[02]))[\V -]?((0?[1-9] (0-2)[0-9]) (3[01]))) (((0?[469]) (11))[\V -]?((0?[1-9] (0-2)[0-9]) (30))) (0?[2] \V-)?(0?[1-9] (0-2)[0-9])))[\V-]?[d]{2,4}\$</code>                                                                                                                                                                                     |
| ISO Dates                  | <code>^((((19 20)(([02468][048]) ([13579][26]))-02-29)) ((20[0-9][0-9]) (19[0-9][0-9]))-(((0[1-9]) (1[0-2]))-((0[1-9]) (1\d) (2[0-8]))) (((0[13578]) (1[02]))-31) (((0[1,3-9]) (1[0-2]))-(29 30))))))\$</code>                                                                                                                                                          |

| Preset Option     | Regular Expression                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Date and Time     | <code>^(?=\d){?:{?:31{?!{?:0?[2469]11}} <br/> {?:30 29}{!0?2} <br/> 29{?.0?2.{?:{?:1[6-9]2-9\d}?<br/> {?:0[48][2468][048][13579][26]} <br/> {?:{?:16[2468][048][3579][26]00}}{?:\x20\$}} <br/> {?:2[0-8]1\d 0?[1-9]})([-./]{?:1[012] 0?[1-9]}\1<br/> {?:1[6-9]2-9\d}?d\d{?:\x20\d\x20\$})?<br/> (((0?[1-9]1[012])(:[0-5]\d){0,2}(\x20[AP]M)) <br/> ([01]\d 2[0-3])(:[0-5]\d){1,2})?\$</code>                                   |
| Time              | <code>^((((0?[1-9]1[0-2])(:\.)([0-5][0-9])(:[.)([0-5][0-9])?<br/> [ ]?(AM am aM Am PM pm pM Pm)) <br/> ((0?[0-9]1[0-9]2[0-3])(:\.)([0-5][0-9])(:[.)([0-5][0-9])?)?)\$</code>                                                                                                                                                                                                                                                   |
| Valid Credit Card | <code>[4\d{12}] (((4 3)\d{3}) (5[1-5]\d{2}) <br/> (6011))(-?\040?)\d{4}(-?\040?){3} <br/> ((3[4,7]\d{2}) ((-?\040?)\d{6}(-?\040?)\d{5})) <br/> (3[4,7]\d{2}) ((-?\040?)\d{4}(-?\040?)\d{4}(-?\040?)\d{3}) <br/> (3[4,7]\d{1}) ((-?\040?)\d{4}(-?\040?){3} (30[0-5]\d{1} <br/> (36 38)\d{2}) ((-?\040?)\d{4}(-?\040?)\d{4}(-?\040?)\d{2}) <br/> ((2131 1800) ((2014 2149)) ((-?\040?)\d{4}(-?\040?)\d{4}(-?\040?)\d{3}))</code> |

Add more expressions to the Regular Expressions **Add Preset** menu by modifying the *RegExPatterns.txt* file located in the Inspector resources folder. This text file is a simple TSV text file. Open the file in a text editor and append the desired expression(s) to the bottom of the file using the following format (separate the words with a TAB).

| Name | Expression | Description | Sample |
|------|------------|-------------|--------|
|------|------------|-------------|--------|

In the upper right corner of the Content pane in the Options section, click **Search** and select **Content only**, **Content and File Names**, or **File Names only** as necessary. Inspector searches for keywords and regular expressions in the contents of a file, in the file name, or both. The Content Only option is selected by default.

Select the following additional search criteria options by activating any or all corresponding checkboxes.

- Case Sensitive
- Unicode (UTF16)
- Skip Files Larger Than
- Report Only First Hit on File

Mark the **Case Sensitive** checkbox to make a keyword search case sensitive. Unmark the **Unicode (UTF 16)** checkbox to ignore unicode or UTF 16 characters. Mark the **Skip Files Larger Than** checkbox and specify a file size to search for files over a specific size. Mark the **Report Only First Hit on File** to stop the search after the first keyword hit.

When you activate the **Deep Search** option, Inspector expands container files, archive files, database files, multimedia files, etc., so the search function can look inside these files for examiner-defined keywords and RegEx patterns. Inspector will also perform a regular ASCII search function at the same time to maximize all possible search results from case evidence.

By default, Inspector deduplicates search hits across multiple Volume Shadow Copies, returning a hit on the oldest Volume Shadow Copy version if others have the same hash value. If a Volume Shadow Copy and primary file have the same hash, both the primary file and oldest Volume Shadow Copy version will be included in search hits, providing the file modification times differ.

You can change the deduplication setting in the Preferences dialog box for Inspector, on the Options tab. For more information, see [Inspector Preferences or Options](#).

## Saved Content Search Settings

After all search options are set as desired, in the bottom right corner of the Content pane, click **Save Search** to save the current search criteria settings for later use. You can overwrite an existing search to replace it, if necessary.

To confirm the search was saved, in the top right corner of the Content pane, click **Saved Searches** and see whether it is in the list.

You can edit the Saved Searches list. Click **Saved Searches** and select **Edit Saved Searches**. The User Created Searches window appears.

To rename a saved search, click **Rename**. After you type the new name, click anywhere outside the text box or press ENTER. The new name appears in the User Created Searches window.

To remove a search from the list, select the search, and then click **Remove**.

## Applying Filters to a Content Search

You can include a preset file filter or a saved custom file filter as part of search criteria. To do so, from the Search view, click **Search All Files** and choose **Files that Match Filter** or **Files that Don't Match Filter**.

In the **Saved File Filter** list, choose a saved file filter or the current unsaved filter.

## Filtering Search Results

After starting a search, you may also apply a view filter to narrow the search results. If the file filter is not currently shown, click **Show/Hide Filter** (three arrows) below the right side of the toolbar. Show/Hide Filter changes in appearance depending on whether filters are shown or hidden and in use or not.

To the right of **Apply**, click **+ (add)**, and then click **Any**. Now you can choose a filter from the list, which provides options appropriate for the view in use. Repeat this to add more filters.

To remove filters, to the right of the specific filter, click **- (remove)**.

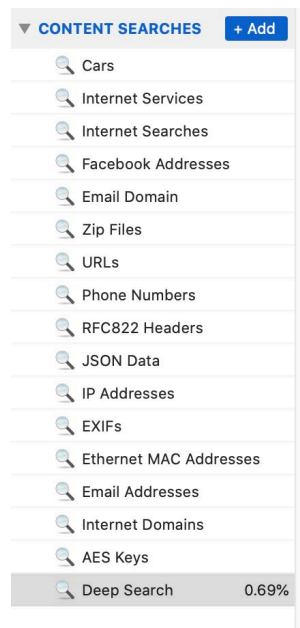
For more information, see [File Filters](#).

## Viewing Content Search Results and Criteria

Click **Start Search**. At the top of the Content pane a progress bar appears. Search results are populated as they are found, and Inspector begins displaying the results while the search is still in progress.

To pause or resume a search, on the right side of the progress bar, click the **Pause/Resume** toggle.

When a search begins, the name of the search and percentage complete indicator appear in the Component list under Content Searches. Click the search name to view the search results.



On the menu bar, choose **View > Adjust List Columns** and select or deselect column options as desired. Selected columns display in the Content pane. The partition column is useful, as it helps the examiner identify which device contains a given hit.

When you export data using the Export Selected Rows feature, Inspector only exports the data in the displayed columns; data in the hidden (unmarked) columns is not exported.

The exception to this rule is the Contacts sub-view in the Communication. From this sub-view, all fields of the contact data, including those seen in the right pane, are included in exports.

In the upper portion of the Content pane, select a file in the file list. The middle section displays a highlighted hit, and a short context snippet for each hit occurrence within the selected file. Double-click on a highlighted keyword and Inspector automatically displays the search hit in the Hex view of the File Content view.

The screenshot shows the Inspector application interface. At the top, there are tabs for Results, Criteria, and Statistics. Below these is a table of search results with columns: BL ID, Name, Path, Keyword, Occurrence, Partition, Version Index, Extension, and Cont. The table lists several files from 'Bennett-Mem.dmp' with keywords like 'josh@2.bing.com' and 'josh@2.bing.com'. Below the table, there is a section for 'Data' with columns: Position, Deep Search, and Context. It shows three data entries, each with a position and a context snippet. The bottom section shows a hex view of the data, with columns for Address, Hex, and ASCII. The hex view displays a large block of hexadecimal data, with some parts highlighted in orange. On the right side, there is a 'Data Interpreter' pane showing a list of data types and their values, including 'String', 'UTF-8', 'Data/Time', 'Chrome', 'Cocoa/Webkit', 'Cocoa/NanoSeconds', 'DOS', 'FILETIME', 'Firefox', 'Java', and 'OLE'.

Each hexadecimal search hit is highlighted in orange. In the bottom right corner under the File Content view, a Selection # indicator appears, along with the hits sector offset, physical sector, logical sector, and cluster start. The Status Bar shows the search hit pathname.

If more than one search hit is returned, click the arrow buttons at the top of the File Content view to navigate through each hit.



You can select and tag search hits from within the File Content view. For more information, see [Tags](#).

With Hex selected, double-click on a highlighted hexadecimal hit. Inspector automatically displays the hit in an appropriate view, such as Media, Internet, and so forth.

To quickly search for another text string within the returned search results, click anywhere in the File Content view, and press your computer's shortcut keys for Find. In the Find window, type the desired text and click **Find**. Any results are highlighted in green.

## Criteria Tab

At the top of the Content pane, click **Criteria** to see the criteria used for the search, the searched partitions, search settings, keywords (including RegEx), and the ignored extensions. Click **Results** to return to the search results.

## Statistics Tab

At the top of the Content pane, click **Statistics** to see search hits for each keyword and total search hits, search size and file count, and the search start, end, and total time elapsed. Click **Results** to return to the search results.

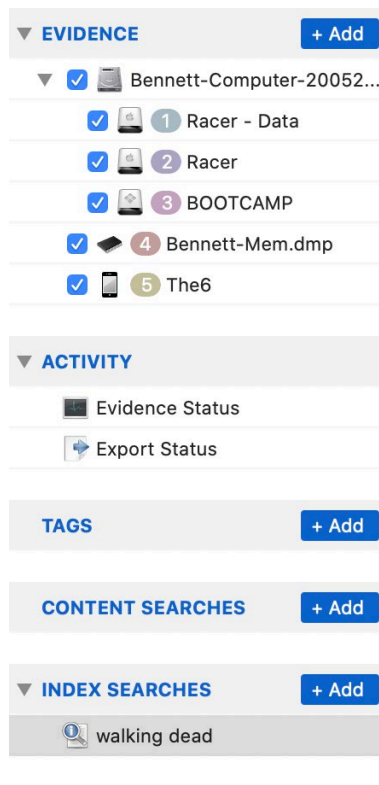
## Index Searching

Inspector provides index capabilities only for allocated files on the file system. These are the files likely to be most relevant for prosecution. Smart Indexing can be run during the initial ingestion of evidence or later.

To run during initial ingestion, select the **Smart Indexing** option when the Evidence item is added. To run Smart Indexing after initial ingestion, navigate to **Evidence Status** and click **Run** next to Indexing.

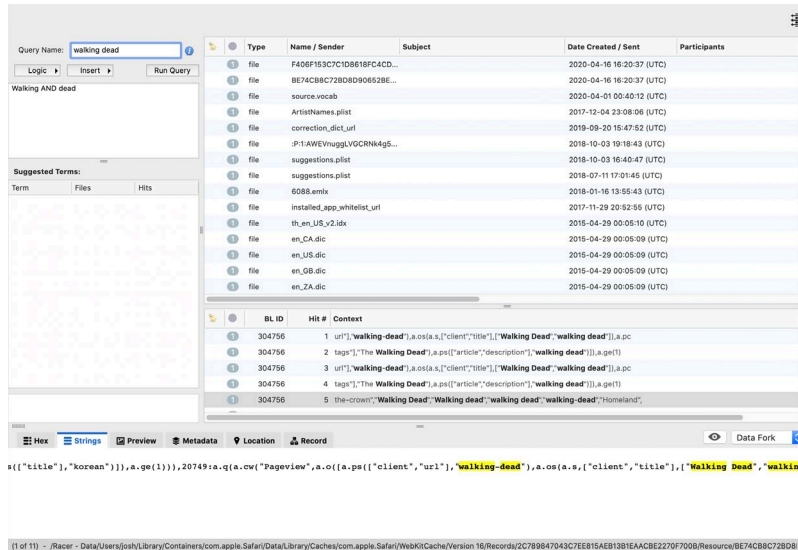
## Creating a Smart Index Query

Once the Smart Index is created, Index Searches can be created in the Component list. To add an Index search, click **Add** next to Index Searches in the Component list.



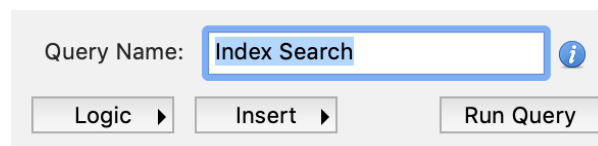
Index Search appears in the Content pane and has areas for these purposes.

- create and execute the query
- display a list of files that match the executed query
- display the highlighted hit

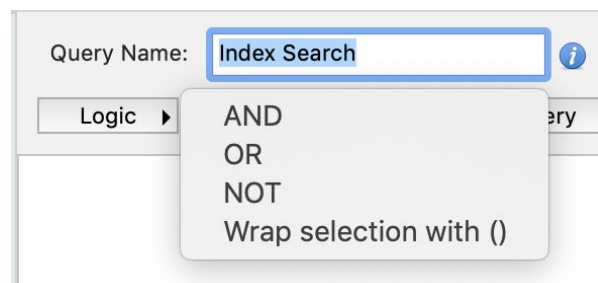


Inspector uses an implementation of SQLite for smart indexing. For more information, see this page: [https://sqlite.org/fts5.html#full\\_text\\_query\\_syntax](https://sqlite.org/fts5.html#full_text_query_syntax).

All new Index Searches have the default Query Name Index Search. This is the name that appears in the Component list for the search. Below the Query Name field are the buttons Logic, Insert, and Run Query.



Click **Logic** to see the logic options.

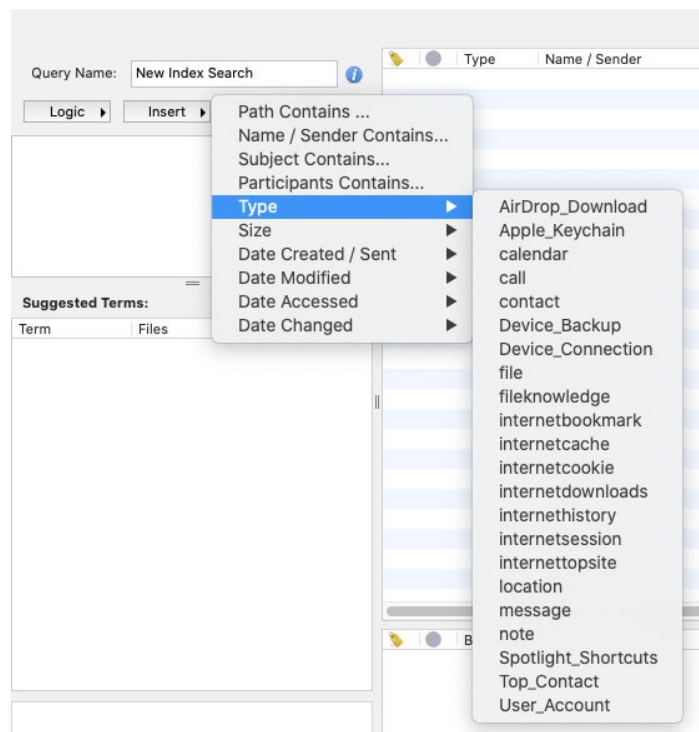


Click **Insert** to see file metadata contained in the Smart Index that can be used to find data of interest.



Data extracted by Inspector from inside of container files (like internet, email, or archives) as a result of processing are included in the index. These metadata fields are available to query the index.

- Path
- Name / Sender Contains
- Subject Contains
- Participant Contains
- Type
- Size
- Date Created
- Date Modified
- Date Accessed
- Date Changed

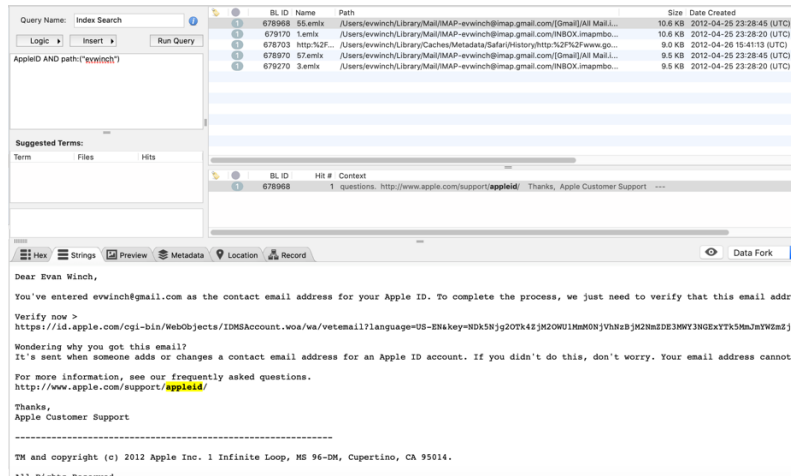


You can use the index to quickly find if a particular topic or subject is mentioned in the evidence set. Indexing the normalized data will return hits for topics or subjects mentioned in internet artifacts, messages and emails, text obtained from optical character recognition (OCR) within image files, or within decompressed archive files.

Indexing can be performed during initial evidence ingestion or performed later from Evidence Status. In this case, indexing occurs after all other processing options.

If indexing is performed before other processes, such as Mail Parsing or Process Archives, once the process runs, the newly processed data will be added to the index. It is common to see Indexing running in Evidence Status each time new information is processed on indexed devices.

To begin building a query, type a search term in the box. Use the Logic operators to combine terms and metadata to create a more complex query. Suggested terms appear in the **Suggested Terms** box as you type, showing the number of hits in the index for each suggested term. Once the query is built, click **Run Query** to see the results. For example, to find information related to a user's AppleID, a query can be created with the word AppleID. To narrow the result to a specific user account, add the metadata Path Contains, entering the user account name in the <pathpart> portion after the AND operator.



The results of the query can be seen in the Content pane. Highlight a result in the list of files returned and the hit is highlighted. The entire file is displayed in the File Content view with the search term hits highlighted. If you highlight multiple files in the list of files returned, multiple hits appear in the highlighted area. If the OCR Image Text process was run against the evidence, OCR text may be returned as a result.

## Bulk Extraction Searches on Memory Files

When you run advanced processing options on a memory file, Inspector uses a bulk extraction tool to perform content searches, scanning the evidence file for key items of interest. These search items are included.

- URLs
- phone numbers
- Internet searches
- .zip files
- JSON data
- ethernet MAC addresses
- AES keys
- email addresses
- Facebook addresses
- Internet services
- email domain
- RFC822 headers
- GPS data
- EXIFs
- Internet domains

Case File

Details

Timeline

Report

Status

Browser

File Filter

Extensions

Cookies

Localizations

Internal

Productivity

System

Plugins

Notifications

ROOTCAMP

Browsers-Mem.dmp

Trust

Tsarshi's Phone

Fore/Intelligence

ACTIVITY

Evidence Status

Export Status

TAGS

Cats

Spotlight

CONTENT SEARCHES

Cats

Spotlight

Cats

Internet Services

Internet Addresses

Personal Mail Addresses

Email Domains

Zip Files

URLs

Phone Numbers

SEC32 Modules

INDEX SEARCHES

Cats

Spotlight

Cats

Internet Services

Internet Addresses

Personal Mail Addresses

Email Domains

Zip Files

URLs

Phone Numbers

SEC32 Modules

RESULTS

CRITERIA

STATISTICS

Browsers-Mem.dmp

Trust

Tsarshi's Phone

Fore/Intelligence

| ID | BL ID   | Name             | Path               | Keyword            | Occurrences | Partition        | Version Index | Extension | Cont |
|----|---------|------------------|--------------------|--------------------|-------------|------------------|---------------|-----------|------|
| 1  | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 3           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 2  | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 2           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 3  | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 3           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 4  | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 2           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 5  | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 3           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 6  | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 1           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 7  | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 1           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 8  | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 3           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 9  | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 1           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 10 | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 4           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 11 | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 1           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 12 | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 3           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 13 | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 1           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 14 | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 1           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 15 | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 | 1           | Browsers-Mem.dmp |               | dmp       | MAC  |
| 16 | 1910813 | Browsers-Mem.dmp | \\Browsers-Mem.dmp | http://192.168.1.1 |             |                  |               |           |      |

**Note:** If a memory evidence item is removed from an Inspector case, the bulk extraction content searches unique to that memory item are removed from the Content Searches section of the Component list.

## Media View

This chapter provides these topics about the Media view in Inspector.

- [Analyzing Picture and Video Files](#)
- [Analyzing Audio Files](#)

## Analyzing Picture and Video Files

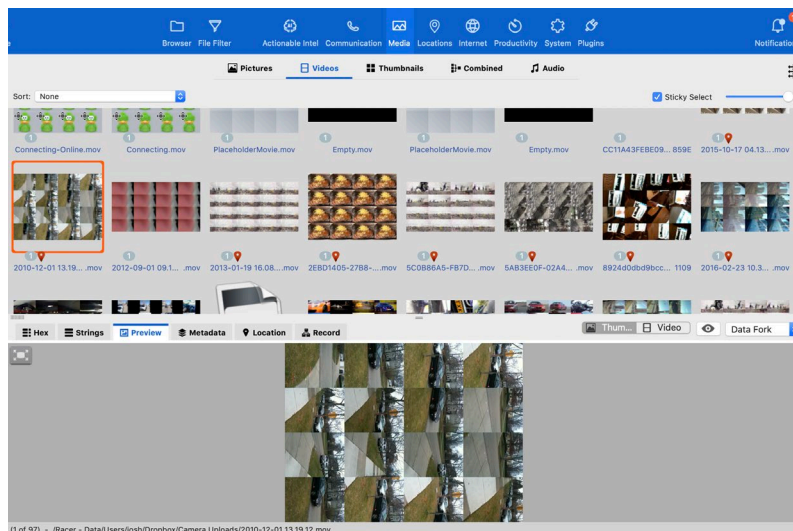
The Media view in Inspector displays a thumbnail gallery of most picture and video files on an evidence item. This view also displays audio file information. Built-in playback controls allow examiners to listen to audio files directly from within Inspector.

The Media view provides options for sorting through visual media files. Select among the Pictures, Videos, or Thumbnails tabs to view those types of files separately or choose the Combined tab to view all three types together.

Picture files and video files are easily discernible from one another in the Media view; video file icons are rendered as 4 x 4 mosaics comprised of sixteen frame-sequence slices.

**Note:** The picture and video thumbnails do not appear if the video and picture processor has not been run.

You can preview video files. To see the video file split into sixteen frame sequences and displayed as a 4 x 4 mosaic, at the top right of the File Content view, click **Thumbs**. If you click **Video**, the video file is rendered with playback controls. To play the video, click **Play**.



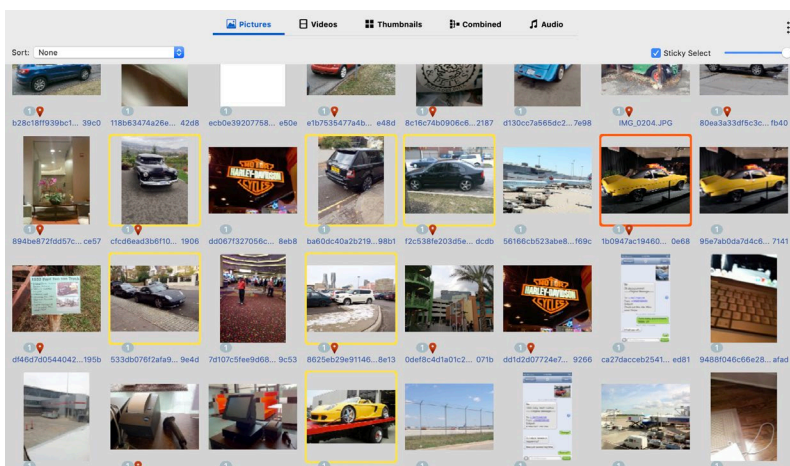
In the Content pane, select a file and press the spacebar, or click **Quick Look** (eye button) to view the file using Quick Look (Mac only). Quick Look displays native Apple application files (and some third-party application files) the same way a user sees them. Audio and video files play within the Quick Look view as well.

**Note:** The Quick Look feature works only when a Quick Look plug-in for the selected file type, or an application that supports the selected file type is installed on the forensic examiners analysis machine.

## Sticky Select

To select and tag multiple pictures or videos, in the top right corner of the Content pane, mark the **Sticky Select** checkbox. Click on several consecutive or non-consecutive pictures and they all remain selected.

To quickly select multiple consecutive pictures in a horizontal and/or vertical row, with Sticky Select enabled, press SHIFT+PAGE UP, +PAGE DOWN, +RIGHT ARROW, or +LEFT ARROW. A red square appears around pictures as they are selected.



To deselect a single picture (and additional non-consecutive single pictures) in one of the selected rows, release the SHIFT key, press and hold CMD or CTRL, and click on the picture.

**Note:** When viewing and scrolling through media, you can press PAGE UP or PAGE DOWN to scroll through full pages of media, rather than scrolling one row at a time with UP ARROW and DOWN ARROW.

In the Media view, a picture or thumbnail that has been recovered from a deleted file is outlined with a red square.

## Thumbnails

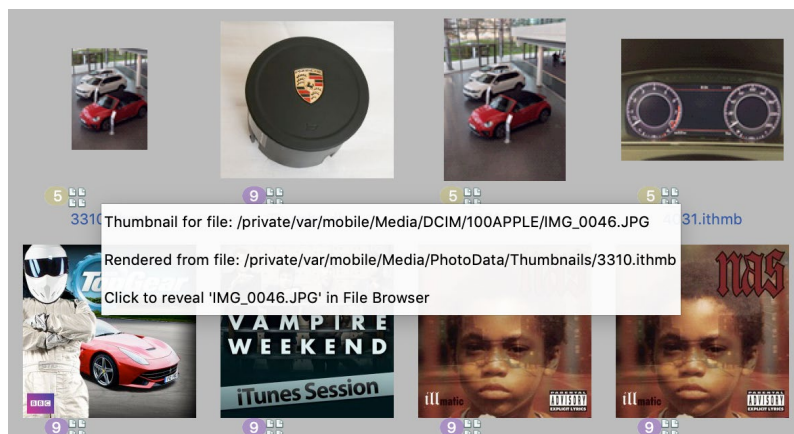
Inspector has the ability to parse thumbnails created for iOS (.ithmb extension), Windows (stored in Thumbs.db files) and macOS (stored in Quick Look's thumbnail cache, *com.apple.QuickLook.thumbnailcache*).

Thumbnails can be viewed in the Media view. Click **Pictures/Videos** to see all pictures and videos, including thumbnails. When a thumbnail is selected in the Content pane, any metadata shown in the File Content view refers to the thumbnail, not its source picture file. Also, double-clicking a thumbnail picture opens the thumbnail, not its source picture file.

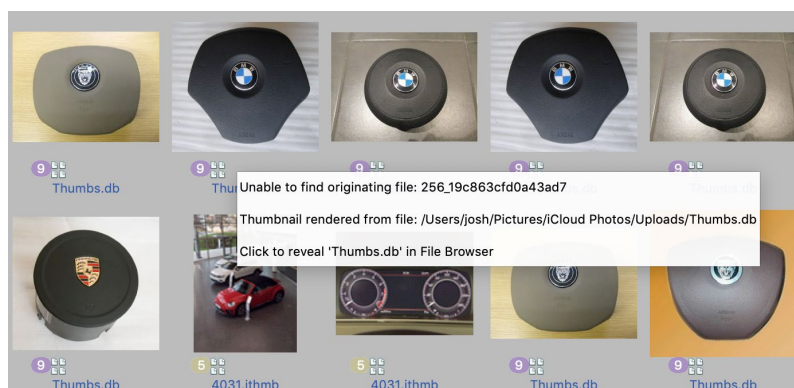
In the Content pane, each thumbnail picture is shown with an icon beneath it.



Hovering the cursor over this icon reveals the path and file name of the thumbnails source file, if it exists. It also indicates the database from which the thumbnail is rendered. Single-clicking the icon reveals the source file in the Browser view.



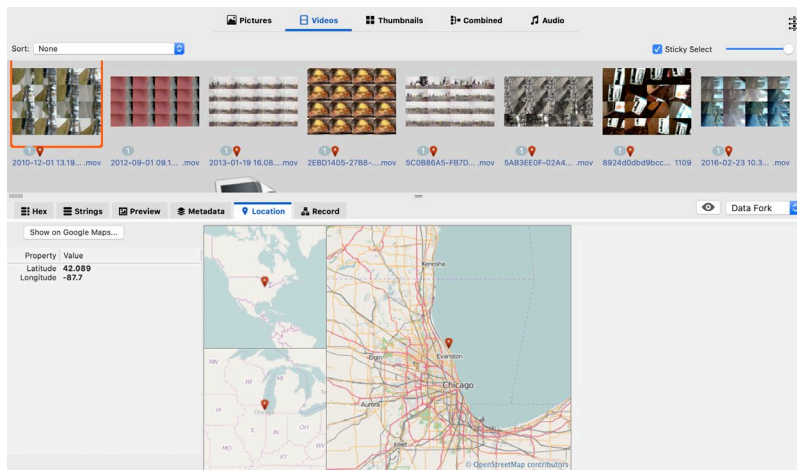
If the source file for a thumbnail is no longer on the system, hovering over the icon will indicate that the source file cannot be located. In such cases, single-clicking the icon reveals the database containing the thumbnail in the Browser view.





## Geolocation Metadata

Picture and video files containing geolocation (GPS) information display with a red placemark icon below the bottom left corner of the file icon. Select a picture or video file that has a placemark icon. At the top of the File Content view, click **Location**. A Mercator map, altitude, altitude reference, latitude, longitude, and timestamp metadata associated with the picture appear.



In the File Content view, click **Show on Google Maps**. Google Maps launches in a default Internet browser window and displays the geolocation information associated with the picture file.

**Note:** The Mercator map feature works on non-networked forensic analysis machines and provides an examiner with general geolocation information. The built-in Google Maps geolocation feature requires an Internet connection and provides an examiner with more exact geolocation information (+/- 5 meters).

## Export Location Data as KMZ or KML

Files containing GPS information can be selected, exported to a .kmz or .kml file, and mapped with the Google Earth application.

1. Select file(s) containing GPS data, click **Action > Export Selected Location Data As**, and then choose either KMZ or KML format.
2. In the Export dialog box, type a file name and choose or create a destination folder, and then click **Export**.  
Inspector exports the GPS data to a .kmz or .kml file in the destination folder.
3. Open the .kmz or .kml file in Google Earth.  
Google Earth displays a pushpin for each file. Each pushpin is also listed in the Google Earth sidebar Places section.

For more information, see [Locating Live Victims](#).

## Image Categorization with Image Analyzer

The integration of Image Analyzer into Inspector provides the capability to run image categorization across pictures and videos. Image Analyzer is a proven solution with years of experience in categorizing images based on the content using machine learning technology. Inspector looks for these categories.

- Alcohol
- Chat: Detects mobile screenshots of messenger applications such as Facebook Messenger, Viber, WhatsApp, Skype, Telegram, and other chat-based applications.
- Child Sexual Abuse Material (CSAM)
- Currency
- Documents
- Drugs
- Extremism
- Gambling
- Gore
- ID/Credit Cards
- Maps
- Porn
- QR & Barcodes
- Swimwear/Underwear
- Vehicles: Detects images containing cars (all types, such as sedans, SUVs, pickups, etc.), trucks, motorbikes, and buses.
- Weapons

Image categorization can reduce review time by revealing images and videos that match a category of interest to the investigation. Examiners can choose which categories to run.

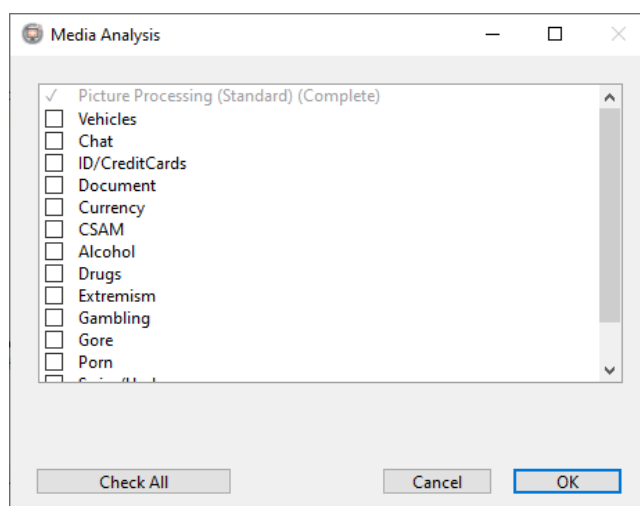
Image Analyzer is completely integrated with Inspector and requires no Internet connection. Improvements to Image Analyzer, including the release of additional threat categories, will be provided with new releases of Inspector. You can request new image categories by sending an email to [support@cellebrite.com](mailto:support@cellebrite.com).

Since Image Analyzer is a learning model, it can be improved when users provide false positives. Reach out to Cellebrite to share false positive images. These images will be directly provided Image Analyzer to refine the model.

Image Analyzer can be run during the initial ingestion of evidence or later. To run during initial ingestion, click the ellipses next to **Picture Analysis** or **Video Analysis**. The Media Analysis dialog box appears.

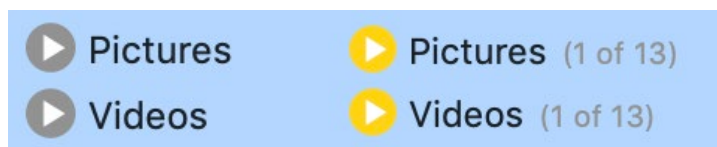
By default, only Standard Processing is selected. To choose all categories, click **Check All**. You can also mark only the necessary categories to run.

Runtime for initial processing with Classify Threat Categories selected may increase significantly.





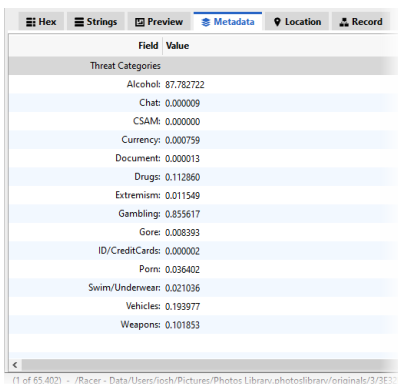
To run Classify Threat Categories after initial ingestion, navigate to the evidence item of interest in Evidence Status. The Play button next to the Pictures and Videos processes is yellow if standard processing or other threat categories have been processed. If nothing was processed, the Play button is gray.



When you click **Play** next to Pictures or Videos, the Media Analysis dialog box appears, where you can choose some or all categories to run.

Video processing in Inspector includes the creation of a 4 x 4 proof sheet containing 16 still frames from across the video. This proof sheet is then classified by Image Analyzer. This is much less time consuming than providing every frame of the video to Image Analyzer, but still allows for more granularity than just providing one frame. Since the proof sheet is composed of 16 snapshots, the classification results for Videos are not as precise as the classification results with Pictures.

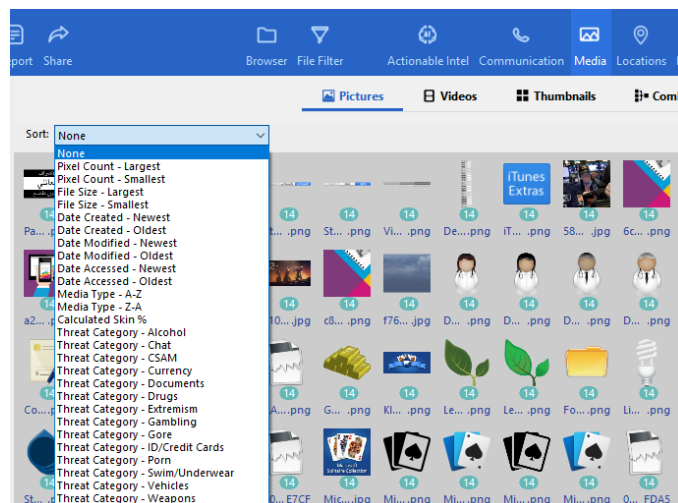
Threat Category results can be seen in the File Information pane or the Metadata tab in File Content view.



Images that are classified have a percentage associated with each threat category. An Image may be associated with more than one threat category. The exception to this is when an image is classified as belonging to one category 100%. In these instances, the image will be classified as only the one category.

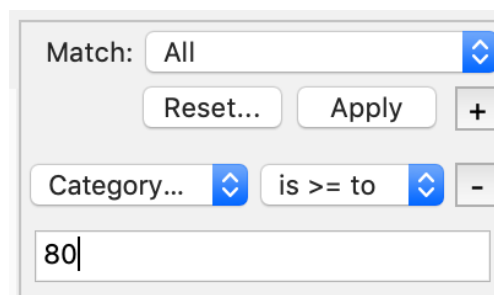
| Threat Categories |         |
|-------------------|---------|
| Alcohol:          | 0.00%   |
| Drugs:            | 0.00%   |
| Extremism:        | 0.00%   |
| Gore:             | 0.00%   |
| Porn:             | 0.00%   |
| Swim/Underwear:   | 0.00%   |
| Weapons:          | 100.00% |

In Media view, content can be sorted by Threat Category.



In Media view, files can also be filtered by Threat Category. In addition to choosing the Threat Category of interest, you can use one of these modifier options.

- is less than
- is greater than
- is between
- is <= to
- is >= to

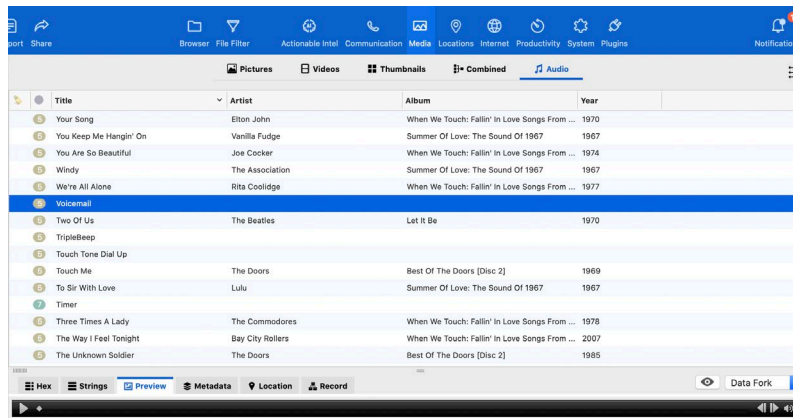


**Note:** The filters will only work with whole numbers.

## Analyzing Audio Files

The Media view shows audio file information and cover art (when available), and built-in playback controls allow examiners to listen to audio files directly from within Inspector.

At the top left of the Content pane, select the drop-down menu, and choose **Audio**. Inspector displays a list of audio files, including music files, ring tones, podcasts, and other sound files, contained on the selected device.



To play an audio file, select it in the Content pane. At the top of the File Content view, click **Preview** and then click **Play**. On Mac computers only, you can also click **Quick Look** (eye button) or press SPACEBAR to play the audio file.

**Note:** iOS application backup files do not store audio information. Therefore, acquire a forensic image or perform a logical acquisition of the connected device if iTunes media is important to the case.

**Note:** Media protected by DRM rights management will not play unless the examiner's machine is authorized.

After you run the metadata processor, you can see audio metadata in the Information pane.



Select a phone, FaceTime, or Skype session file in the Content pane. In the File Content view, click **Preview**.

The File Content view displays the database file containing raw data for calls, FaceTime sessions, and Skype sessions. For iOS devices, this database is the *call\_history.db* SQLite database file, which contains the last 100 communication records sent or received on the iOS device. This is the maximum number of records the *call\_history.db* SQLite database can retain under normal circumstances. If the iOS device is jailbroken, the database file may be customized and may retain more than 100 records.

Inspector displays communication records deleted by the user or the device's operating system in *red italic* font.

## Voicemail

At the top of the Content pane, click **Voicemail**. Voicemail records are displayed. At the top of the File Content view click **Preview**. Select an active voicemail file, and in the File Content view, audio playback controls display. Click **Play** to listen to the voicemail.

If a voicemail number is associated with a contact in the device's address book, a name appears in the Name(s) column. Unheard voicemail records display with a small blue dot in the Unheard column. If an examiner listens to the message from within the Inspector interface, the small blue dot remains.

In the Content pane, highlight a voicemail record and press SPACEBAR. A Quick Look window appears and automatically plays the voicemail message. Or, at the top of the File Content view, click **Preview** to display an audio playback interface for the selected voicemail. Click **Play** to play the voicemail.

Deleted records appear in *red italic* font. In some instances, a record is displayed twice, once as a deleted record and once as an active record. When a caller leaves a voicemail, duplicate records may be created. When the user deletes the voicemail, the iOS operating system only deletes one of the records.

**Note:** Deleted voicemail files do not play back; however, the deleted date displays in the Deleted Date column in the Content pane if a voicemail file is deleted. When a user deletes a voicemail, it is moved to a folder called Deleted Messages. Deleted messages remain in the Deleted Messages folder until the folder is cleared.

Recovered voicemail messages cannot be played. Voicemail messages on iOS are AMR files. When a voicemail is deleted, the AMR file is also deleted. Voicemail files on devices running older iOS versions can sometimes be carved from unallocated space. However, recovery is currently not possible if the device is running iOS version 4 and higher.

**Note:** Deleted voicemail messages are deleted, but not removed from the device. When a user deletes a voicemail, it is moved to the Deleted Messages folder. Until the Deleted Messages folder is cleared, the voicemail remains on the device.

## Voice Memos

At the top of the Content pane, click **Voice Memos**. Voice memo details are displayed. Select a voice memo in the Content pane, and press SPACEBAR. A Quick Look window appears and automatically plays the Voice Memo file. Or, at the top of the File Content view, click **Preview** to display an audio playback interface for the selected voicemail. Click **Play** to play the Voice Memo file.

Like deleted voicemail messages, deleted Voice Memo files appear, but do not play because the .m4a file is deleted from the file system when the voice memo is deleted.

## Favorites

At the top of the Content pane, click **Favorites** to display contacts that a user designates as favorites (possibly the most often used contacts). Favorites data is arranged in Name, Address (number), and Label (home, mobile, work, etc.) columns.

## Messaging

Inspector parses and displays these types of message communication.

- SMS
- MMS
- iMessage
- iChat
- Skype
- Messages
- WhatsApp
- Kik
- textPlus
- Textfree
- Tango

In the Component list in the Evidence section, select a device. On the toolbar, click **Communication**, then click **Messages**. Every messaging service that can be parsed by Inspector will appear in the main window.

Inspector displays communication records deleted by the user or the device OS in *red italic* font.

**Note:** Deleted SMS messages are often incomplete. Inspector attempts to look up related participants and content from the non-deleted record set to present a more complete message. Examiners should be aware that the relationship between a deleted record and non-deleted content may be erroneous.

| Service | Direction | Date                      | Content                                                        | Subject | Sender                           | Participants                     | Attachment |
|---------|-----------|---------------------------|----------------------------------------------------------------|---------|----------------------------------|----------------------------------|------------|
| SMS     | Outgoing  | 2010-11-29 02:06:18 (UTC) | To                                                             |         | Self ( (245) 484-6399 )          | A Dog ( (847) 736-9491 )         |            |
| SMS     | Outgoing  | 2010-11-29 02:06:18 (UTC) | To                                                             |         | Self ( (245) 484-6399 )          | A Dog ( (847) 736-9491 )         |            |
| SMS     | Outgoing  | 2010-11-30 19:33:57 (UTC) | Ha, this is the fool who left there phone in the car. Mine now |         | Self ( (245) 484-6399 )          | A Dog ( (847) 736-9491 )         |            |
| SMS     | Outgoing  | 2010-11-30 19:33:57 (UTC) | <attachment - image.jpg - 2-0.jpg>                             |         | Self ( (245) 484-6399 )          | A Dog ( (847) 736-9491 )         |            |
| SMS     | Outgoing  | 2010-11-30 19:33:57 (UTC) | Ha, this is the fool who left there phone in the car. Mine now |         | Self ( (245) 484-6399 )          | A Dog ( (847) 736-9491 )         |            |
| SMS     | Incoming  | 2010-11-30 19:37:12 (UTC) | No way man. Make sure you watch yourself, but that's awesome!  |         | A Dog ( (847) 736-9491 )         | A Dog ( (847) 736-9491 )         |            |
| SMS     | Incoming  | 2010-11-30 19:37:12 (UTC) | No way man. Make sure you watch yourself, but that's awesome!  |         | A Dog ( (847) 736-9491 )         | A Dog ( (847) 736-9491 )         |            |
| SMS     | Outgoing  | 2010-11-30 19:39:40 (UTC) | Look at my old dumb phone. Going straight in the trash         |         | Self ( (245) 484-6399 )          | A Dog ( (847) 736-9491 )         |            |
| SMS     | Outgoing  | 2010-11-30 19:39:40 (UTC) | Look at my old dumb phone. Going straight in the trash         |         | Self ( (245) 484-6399 )          | A Dog ( (847) 736-9491 )         |            |
| SMS     | Outgoing  | 2010-11-30 19:39:40 (UTC) | Look at my old dumb phone. Going straight in the trash         |         | Self ( (245) 484-6399 )          | A Dog ( (847) 736-9491 )         |            |
| SMS     | Incoming  | 2010-11-30 19:41:57 (UTC) | Wow. For sure an upgrade.                                      |         | A Dog ( (847) 736-9491 )         | A Dog ( (847) 736-9491 )         |            |
| SMS     | Incoming  | 2010-11-30 19:41:57 (UTC) | Wow. For sure an upgrade.                                      |         | A Dog ( (847) 736-9491 )         | A Dog ( (847) 736-9491 )         |            |
| SMS     | Outgoing  | 2010-11-30 22:39:25 (UTC) | I'm on fire. Check out this apple tv i just jacked             |         | Self ( (245) 484-6399 )          | Lar Schwenker ( (847) 687-8188 ) |            |
| SMS     | Outgoing  | 2010-11-30 22:39:25 (UTC) | I'm on fire. Check out this apple tv i just jacked             |         | Self ( (245) 484-6399 )          | Lar Schwenker ( (847) 687-8188 ) |            |
| SMS     | Outgoing  | 2010-11-30 22:39:25 (UTC) | I'm on fire. Check out this apple tv i just jacked             |         | Self ( (245) 484-6399 )          | Lar Schwenker ( (847) 687-8188 ) |            |
| SMS     | Outgoing  | 2010-11-30 23:02:24 (UTC) | It's sweet. Watching fast and furious on it now                |         | Self ( (245) 484-6399 )          | Lar Schwenker ( (847) 687-8188 ) |            |
| SMS     | Outgoing  | 2010-11-30 23:02:24 (UTC) | It's sweet. Watching fast and furious on it now                |         | Self ( (245) 484-6399 )          | Lar Schwenker ( (847) 687-8188 ) |            |
| SMS     | Incoming  | 2010-11-30 23:03:11 (UTC) | Nice                                                           |         | Lar Schwenker ( (847) 687-8188 ) | Lar Schwenker ( (847) 687-8188 ) |            |
| SMS     | Incoming  | 2010-11-30 23:03:11 (UTC) | Nice                                                           |         | Lar Schwenker ( (847) 687-8188 ) | Lar Schwenker ( (847) 687-8188 ) |            |

Full Message:  
Ha, this is the fool who left there phone in the car. Mine now

To filter messages by contacts, at the top of the Content pane, choose Contacts in the **Filter** field. The default is All messages. To sort messages, click **List View** and then click a column heading by Service, Direction (incoming or outgoing), Date, Content, Subject, Sender, Participants, and so forth.

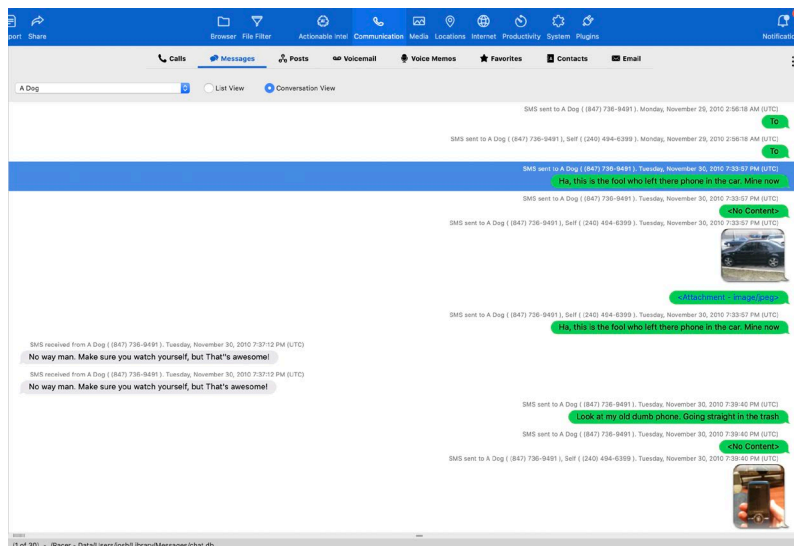
Message records are easily sorted and tagged using these filter and sort features. In List View, selecting a message causes the message contents to appear in the Full Message panel in the lower section of the Content pane.

**Note:** Messages without text appear in the List View with an empty Content column.

In the Content pane, select an MMS message. In the File Content view, click **Preview**. Items that display as Attachment indicates that a file is attached to a message. These may be pictures, movies, or other file types, and the type will be indicated next to the word Attachment. For instance, an attached image would show <Attachment - image/filename> in the Content column.

You can see a message as a two-way conversation, the way a user would actually see it on a device. At the top of the Content pane, click **Conversation View**. Picture files display as thumbnails, and movie files display with a play icon superimposed over a static thumbnail within the conversation.

Conversation View shows messages using three different conversation bubble colors: green for outgoing SMS messages, blue for outgoing iMessages, and gray for incoming messages (the same way an iOS device displays them). The colors are the same for other messaging types.



Media files may be viewed and/or played (if the file is a movie) in the File Content view using the Preview or Quick Look views.

Scroll through the Hex, Strings, Preview and Quick Look (Mac only) tabs at the top of the File Content view to examine SMS, MMS, and iMessage records using different views. Select a message containing a movie file. In the File Content view, click **Preview**. Click **Play** in the File Content view, or click **Quick Look** (eye button), and the movie plays.

MMS movies usually have the file extension of .3gp and are located in the */Library/SMS/Parts* directory (folder). Use the File Filter to quickly find and view MMS and iMessage movies. For more information, see [File Filters](#).

If iChat log files are present, they are represented by the messaging service that was used. The name of the particular messaging service used will appear in the Service column. For example, if AIM was used for iChat, the name AIM will be listed in the Service column. Other iChat messaging services include Google Talk and JABBER.

Select an AIM item in the Content pane. In the File Content view, click **Preview**. The chat session .plist data, created by the iChat application, is displayed. iChat sessions are stored in a .plist file.

In the File Content view, click **Hex**, **Strings**, **Preview** and **Metadata** to display iChat data in different ways.

**Note:** Inspector only shows the first 63 fields (columns) for each database record. If an examiner selects a table with more than 63 fields, a warning dialog appears to let the examiner know that some fields (columns) are not displayed.

## Social Media

Inspector parses and displays communications from several common social media applications. In the Evidence section of the Component list, select a device. On the toolbar, click **Communication > Posts**. Select any column in the Content pane to sort.

Communications from all social media applications are shown together in the Content pane. Select an item, and the full text of the message appears in the Full Post display area beneath the Content pane. Inspector displays communication records deleted by the user or the device's operating system in *red italic* font.

The Posts sub-view can show this information, when it is available, about each post in the Content pane.

| Column  | Description                              |
|---------|------------------------------------------|
| Service | Name of the social media application     |
| Date    | Post timestamp                           |
| Post ID | The application's ID number for the post |
| Title   | Title text of the post                   |
| Post    | Body text of the post                    |
| Comment | Comment text of the post                 |



| Column           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Media            | [blank] - No media item was attached to this post<br><Attachment - image> / <Attachment - photo url> - A media item was attached to this post                                                                                                                                                                                                                                                                                                           |
| Author           | The author of the post<br>If the author cannot be identified, this value shows Unknown.                                                                                                                                                                                                                                                                                                                                                                 |
| Media Owner      | The media owner of the media attached to the post                                                                                                                                                                                                                                                                                                                                                                                                       |
| Associated Users | Users associated with the post                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Comment Link ID  | <ul style="list-style-type: none"> <li>For Foursquare posts containing a comment entry, this value identifies the ZFSCOMMENT table row from the Foursquare app's <i>foursquare.sqlite</i> database where the comment text was identified</li> <li>For Facebook fragments containing a comment entry, this value identifies the ZCOMMENT table row from the Facebook app's <i>Store.sqlite</i> database where the comment text was identified</li> </ul> |
| Media Link ID    | <ul style="list-style-type: none"> <li>For Foursquare posts containing a media entry, this value identifies the ZFSPHOTO table row from the Foursquare app's <i>foursquare.sqlite</i> database where the media entry was identified</li> <li>For Facebook fragments containing a media entry, this value identifies the ZMEDIA table row from the Facebook app's <i>Store.sqlite</i> database where the media entry was identified</li> </ul>           |

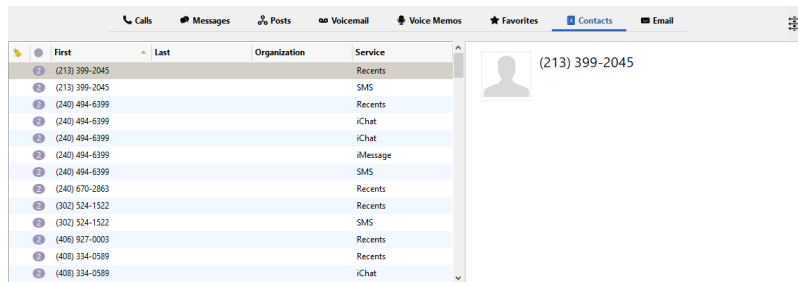
Post fragments with an associated picture may have a locally cached version of that picture. If a locally cached version exists and is able to be identified, Inspector parses and displays that picture in Preview sub-view when the fragment is selected.

To focus on items from just one application (such as Facebook, Foursquare, Swarm, Twitter, LinkedIn, or Tango), sort by the Service column or use a filter. To show or hide the file filter, click **Show/Hide Filter** (three arrows) below the right side of the toolbar. Then select the desired filter to narrow results. For more information, see [File Filters](#).

You can see application bundle contents, including available profile information for social media applications. For more information, see [System View](#).

## Contacts

On the toolbar, click **Communication > Contacts**. This sub-view shows contacts on a device.



On the left side of the Content pane select a contact, and on the right side of the Content pane select a contact avatar if one exists. The source image opens to its full size. Contact avatars are sometimes cropped or masked. By selecting the avatar in Inspector, you can see the entire source image. Tag the image, and it will appear in a report both as a thumbnail and as a full-size image.

Deleted contacts appear in *red italic* font.

Records in the Contacts sub-view can be exported as either tab-delimited or CSV files. In the left side of the Content pane, select one or more rows of data, open the context menu, and then click **Export > Export Selected Rows** to choose the format (tab-delimited or CSV) and save location. All fields of the contact data are included in exports, meaning all data in the right half of the Content pane, rather than just the first name, last name and organization fields seen in the highlighted row. Contacts with multiple entries of the same type (for example multiple email addresses) have those entries combined into a single field on the export, with semicolons used to separate entries.

| Phone(s)       | Email(s)                           | Location | Other Data                  |
|----------------|------------------------------------|----------|-----------------------------|
| (408) 513-1851 | max@peplemovers.net;maxw@gmail.com |          |                             |
| (202) 867-8156 | pauls@psi.net                      |          | HomePage:www.psi.net        |
|                |                                    |          | Skype ID:makayla_shakeit;Bt |

## Email

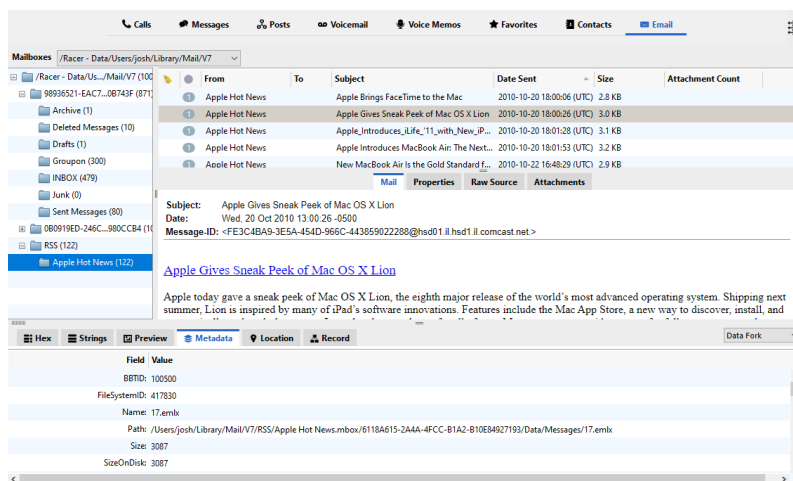
The Email sub-view in Inspector supports these email formats.

- .pst and .ost (Outlook for Windows)
- general mbox (exported Mac Mail and other platform-agnostic clients)
- .olk15Message (Outlook for Mac)
- .eml
- .emlx
- .imapmbox

For an email to be included in a report and viewable as the user saw it, you must tag the email from this Email sub-view.

1. In the Evidence section of the Component list, select an evidence item.
2. On the toolbar, click **Communication > Email**.
3. At the top of the Content pane, click **Mailboxes** and choose a mailbox to view, or leave the drop-down set to All.

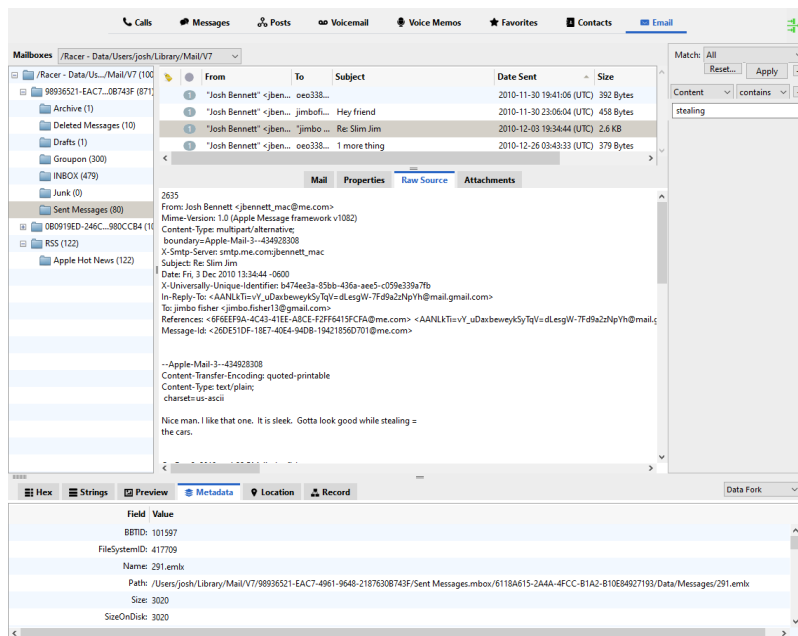
Unread emails are shown in bold text. Emails that have one or more attachments show the quantity in the Attachment Count column.



To find a keyword within of any parsed mail messages, use the filter on the far right in the Communication view. These are filter options for email.

- Attachment Count
- Date Sent
- From
- Subject
- Size
- To
- Content

Filtering by content looks for data within the content of the emails.



When you select an email in the list, these tabs in the lower portion of the Content pane allow for various views of that email.

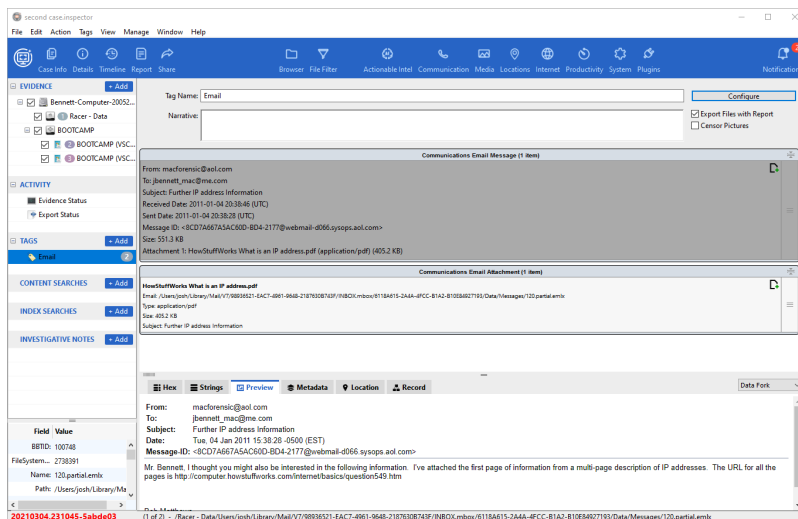
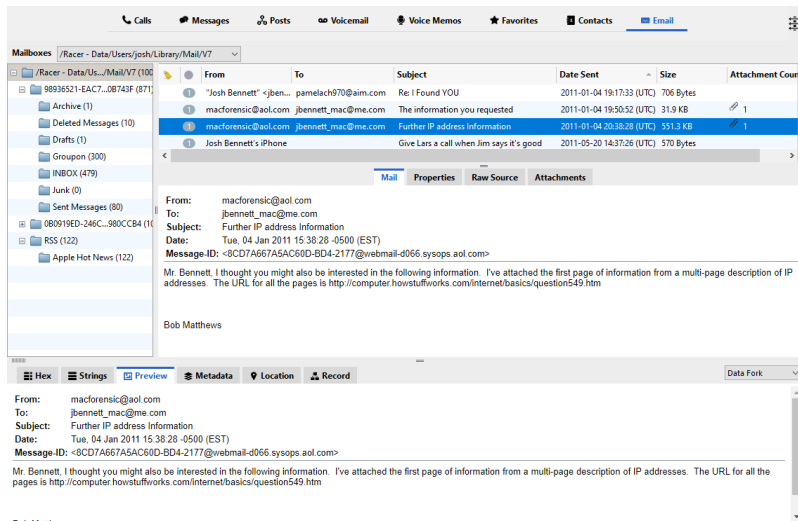
- Mail (for a rendering of the email)
- Properties
- Raw Source
- Attachments (to see a list of attachments)

Choose an attachment, then click **Preview** in the File Content view. The selected file appears. On Mac computers, with the attachment file still selected, click **Quick Look** (eye button) or press SPACEBAR to see the attachment using the Quick Look framework. Email attachments are tagged with the email and can also be tagged separately.

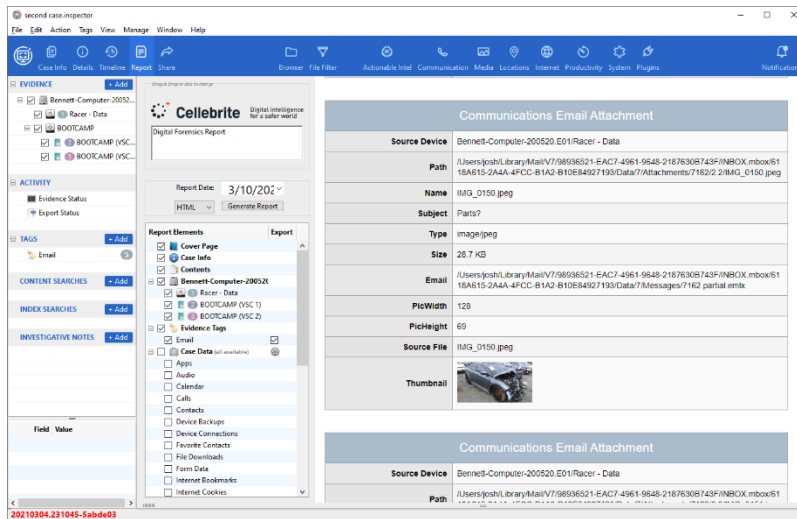
For more information, see [Tags](#).

## Support for EMLX and EMLX Partial


EMLX is a Mail Message (Apple Mail Email) file used to store an email message. These are plain text files that store just a single email message. EMLXPART files are used by Apple Mail as well, but as attachment files instead of as the actual email files. The emails show the typical context instead of the header information and the attachments are automatically included.



To render the attachments in the report, you must enable the preference to Create previews for tagged email. It is disabled by default because it can slow down generation of very large reports. For more information, see [Inspector Preferences or Options](#).



When the report is generated, the email can be seen as well as previewed by clicking on the Preview link. This shows the email as the user saw it. Any attachments can also be seen in the preview of the report as well as the attachment link.

| Email                         |                                                                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Email</b>                  |                                                                                                                                                    |
| <b>Source Device</b>          | Bennett-Computer-APFS-180208.E01/Racer                                                                                                             |
| <b>Path</b>                   | /Users/josh/Library/Mail/V5/98936521-EAC7-4961-9648-2187630B743F/INBOX.mbox/6118A615-2A4A-4FCC-B1A2-B10E84927193/Data/3/Messages/3513.partial.emlx |
| <b>From</b>                   | godzillin@me.com                                                                                                                                   |
| <b>To</b>                     | a.donnie01@gmail.com> Josh Bennettjbennett_mac@me.com                                                                                              |
| <b>Subject</b>                | Mail                                                                                                                                               |
| <b>Received Date</b>          | 2015-12-23 19:30:46 (UTC)                                                                                                                          |
| <b>Sent Date</b>              | 2015-12-23 19:30:39 (UTC)                                                                                                                          |
| <b>Message ID</b>             | <2F7F73DB-E9FC-4B97-AAF5-EBE89A72DAD0@me.com>                                                                                                      |
| <b>Body</b>                   | Might be a new place to hang.                                                                                                                      |
| <b>Size</b>                   | 516.4 KB                                                                                                                                           |
| <b>Source File</b>            | <a href="#">3513.partial.emlx</a>                                                                                                                  |
| <b>Preview</b>                | <a href="#">Mail</a>                                                                                                                               |
| <b>Attachment 1</b>           | <a href="#">IMG_0391.PNG (image/png) (375.8 KB) (w. 72 h. 128)</a>                                                                                 |
| <b>Attachment 1 (Preview)</b> |                                                                 |

| Email                |                                                                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source Device</b> | Bennett-Computer-APFS-180208.E01/Racer                                                                                                          |
| <b>Path</b>          | /Users/josh/Library/Mail/V5/98936521-EAC7-4961-9648-2187630B743F/INBOX.mbox/6118A615-2A4A-4FCC-B1A2-B10E84927193/Data/Messages/607.partial.emlx |
| <b>From</b>          | g.fault.gibson@gmail.com                                                                                                                        |
| <b>To</b>            | jbennett_mac@me.com                                                                                                                             |
| <b>Subject</b>       | Secret                                                                                                                                          |
| <b>Received Date</b> | 2012-08-22 12:29:54 (UTC)                                                                                                                       |
| <b>Sent Date</b>     | 2012-08-22 12:28:31 (UTC)                                                                                                                       |
| <b>Message ID</b>    | <CACgOffcWVFDQL5CdVAnxwa9GjdaGm37sCGGqdTnO1Z40GZ_BO@mail.gmail.com>                                                                             |
| <b>Body</b>          | Here you go...what you've been waiting for. Usual password.                                                                                     |
| <b>Size</b>          | 13.8 MB                                                                                                                                         |
| <b>Source File</b>   | <a href="#">607.partial.emlx</a>                                                                                                                |
| <b>Preview</b>       | <a href="#">Secret</a>                                                                                                                          |
| <b>Attachment 1</b>  | <a href="#">Things.dmg (application/octet-stream) (0 Bytes)</a>                                                                                 |

**From:** Taz Zillin <godzillin@me.com>  
**To:** Donnie Adams <a.donnie01@gmail.com>, Josh Bennett <jbennett\_mac@me.com>  
**Subject:** Mail  
**Date:** Wed, 23 Dec 2015 11:30:39 -0800  
**Message-ID:** <2F7F73DB-E9FC-4B97-AAF5-EBE89A72DAD0@me.com>

Might be a new place to hang.

## Locations, Internet, and Productivity Views

This chapter provides these topics about the Locations, Internet, and Productivity views.

- [Locations View](#)
- [Internet View](#)
- [Productivity View](#)

### Locations View

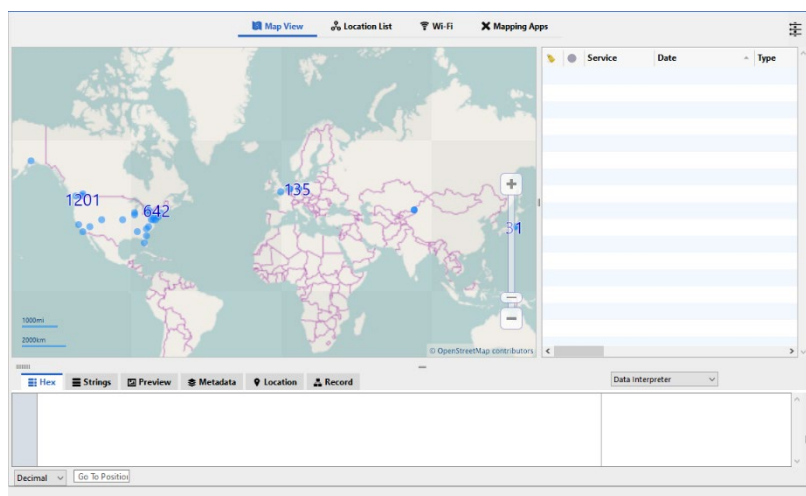
In the toolbar, click **Locations** to open the Locations view. The Locations view lets you examine this information.

- Google and Apple Maps usage
- Geolocation data from media files, calendar and social media apps
- Wi-Fi network information
- Additional location services data. This is Apple's definition of location services.

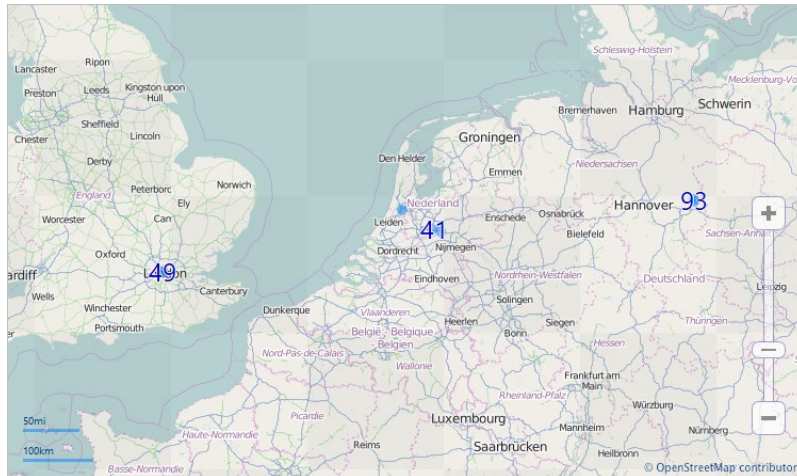
*"Location Services allows location-dependent apps and websites (including Maps, Camera, Safari, and other Apple and third-party apps) to use information from cellular, Wi-Fi, and Global Positioning System (GPS) networks to determine your approximate location."*

### Map View Sub-view

The default sub-view in Locations is Map View. This view assembles all of the location data parsed from the evidence, creating an interactive cluster map. Location data parsed includes Google Maps and Apple Maps searches, bookmarks, dropped pins, and old tags, as well as media files and calendar items that contain geolocation data. Also, certain social media apps contain geolocation data that can be parsed into this sub-view. While each app may store different pieces of data, at a minimum, latitude and longitude are parsed and displayed. Based on the source app, additional information such as a timestamp, location name and address, and other data may be parsed and displayed. The map is generated using map tiles installed on the system with the Inspector installer based on OpenStreetMap. All data containing geolocation information is represented on the cluster map by a blue dot. Densely populated regions of the map also display a numerical value indicating the number of data items mapped in that region.



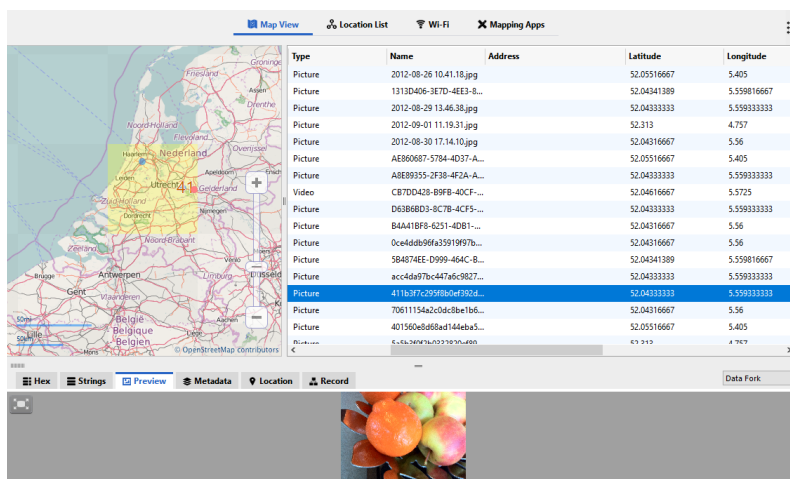
The cluster map lets you zoom in and out using the slide bar on the lower right side. When zooming, it automatically focuses on the area of the map centered in the window. To change the focus, click of the map window, hold down the mouse button and drag the appropriate region into the center of the map. You can do this as necessary until the appropriate region is shown in the center of the map.



Map tile sizes change when the zoom level changes. Interacting with the map tiles reveals the mapped geolocation data. When a map tile is selected, data points mapped on that tile appear in the right side of the Content pane. These columns can provide detailed information.

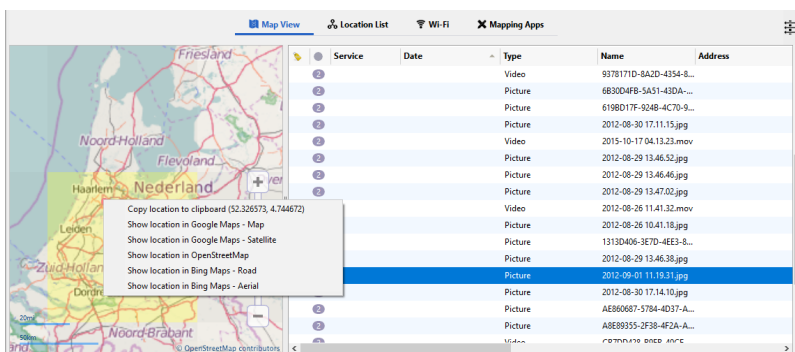
- Service
- Date
- Type
- Name
- Address
- Latitude
- Longitude
- Distance
- Altitude
- Accuracy
- Speed

The selected map tile is highlighted on the map in the Content pane with the corresponding data listed on the right side of the pane. Data points are marked on the map with a blue dot. If a data point is selected on the map, the dot changes to pink and the corresponding data on the right is highlighted.



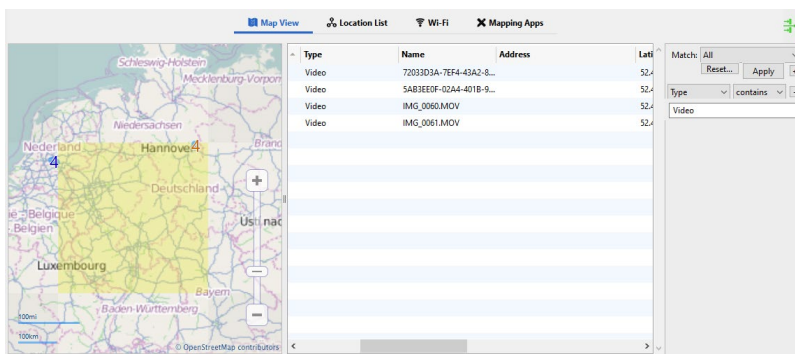


For a data point on the map, open the context menu, where you can copy the location to the clipboard, or show the location in Google Maps, OpenStreetMaps, or Bing Maps. When connected to the Internet, choosing an option for showing location opens the selected map in the default web browser.



Tagging information from Map View tags only the location data. It does not tag the associated file or any other file metadata. You can tag the file only in the Browser view. To see the file associated with location data, open the context menu from an item in the list, and then click **Reveal > File in File Browser**.

You can use the Filter pane in the Map View to show geolocation information based on the parsed data. For instance, you can create a filter to map only geolocation data extracted from Video data. Once a filter is applied, the cluster map shows only the data that meets the filter criteria.



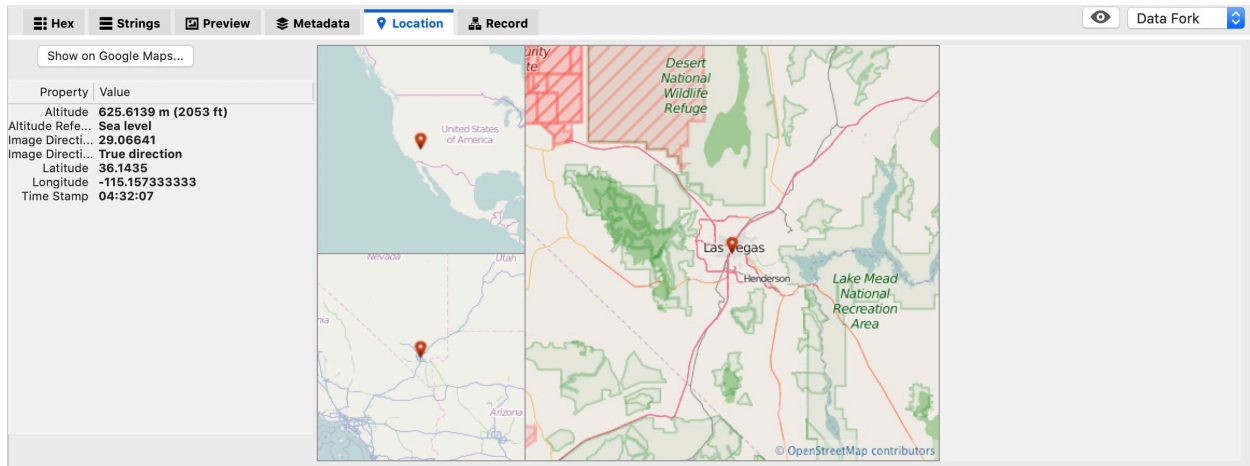
## Location List Sub-view

At the top of the Content pane, click **Location List**. The Location List sub-view displays Google Maps and Apple Maps searches, bookmarks, dropped pins, old tags, as well as media files and calendar items that contain geolocation data. Also, certain social media apps contain geolocation data that can be parsed into this sub-view. While each app may store different pieces of data, at a minimum, latitude and longitude are parsed and displayed. Based on the source app, additional information such as a timestamp, location name and address, and other data may be parsed and displayed.

Select any record in the Location List view, then click **Location** in the File Content view to see one or more offline maps depicting the item's latitude and longitude coordinates.

## Offline Maps

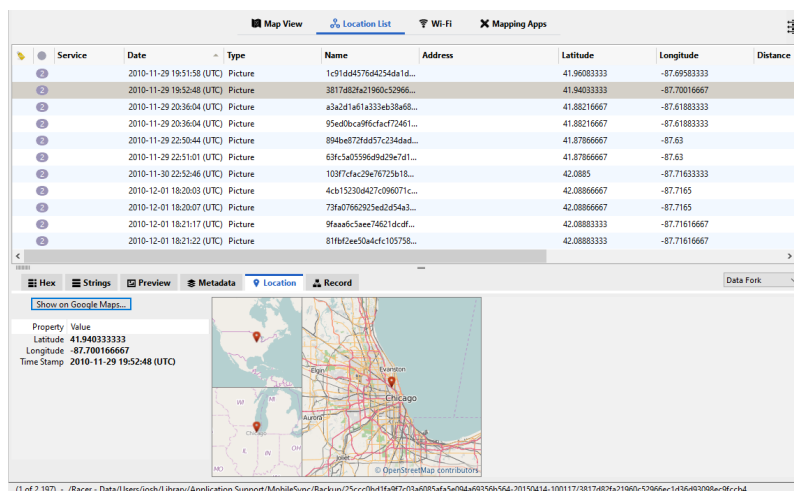
Inspector presents a set of static maps based on OpenStreetMap. Select a file that contains GPS coordinates and click **Location** in the File Content view. In the Location tab, you can see an offline map with three levels of zoom. You can download additional maps for additional zoom capabilities.



The zoom is currently set at levels 3, 5, and 8. When additional zoom level tiles are downloaded, Inspector increases its maximum zoom accordingly. When connected to the Internet, you may also zoom in by clicking **Show on Google Maps**.

The default web browser opens to Google Maps, allowing control of the zoom level and viewing style. With Inspector, you can export files containing GPS information as a .kmz file or in .kml format.

Select the files containing GPS data, open the context menu, click **Export > Export Selected Location Data As**, and then choose either KMZ or KML format. In the Export window, provide a file name, choose or create a destination folder, and then click **Export**. Inspector exports the GPS data to a .kmz or .kml file in the destination folder. To see the geolocation coordinates using Google Maps, click **Show on Google Maps**. (The analysis machine must be connected to the Internet.)



For iOS devices, the Location Data sub-view also displays the *consolidated.db* file (Location Services) contents here: */Library/Caches/locationd/consolidated.db*.

**Note:** iOS versions 4.3.3 and later no longer store GPS coordinates in this database.

For Location Services, three data types are displayed: Wi-Fi, Cell and Cell (Local). Wi-Fi information is collected from nearby Wi-Fi access points. Cell data is collected from nearby cell towers.

Cell (Local) is data from cell towers the phone connects to. This data may suggest the phone's locations over time. Date and timestamp data is not always accurate, however, because Apple batch dumps much of this data into this database. Look at the timestamps and notice they are often the same.

Each database record includes the type of Location Service (Wi-Fi or Cell), a UTC timestamp, and GPS latitude and longitude coordinates. If Location Services obtained geolocation data from a Wi-Fi signal, the Wi-Fi device Media Access Control (MAC) address appears.

Geolocation data in the Location Data sub-view may be exported from a non-networked analysis machine to a networked machine and viewed dynamically using the Google Earth application. In the Content pane, use your computer's normal procedures to select a single record, several adjacent records, or several non-adjacent records. Open the context menu, select **Export Selected Location Data As**, then choose either KMZ or KML format. In the Export window, provide a name for the file, choose or create a destination folder, and then click **Export**. Inspector exports the GPS data to a .kmz or .kml file in the destination folder.

## Wi-Fi Sub-view

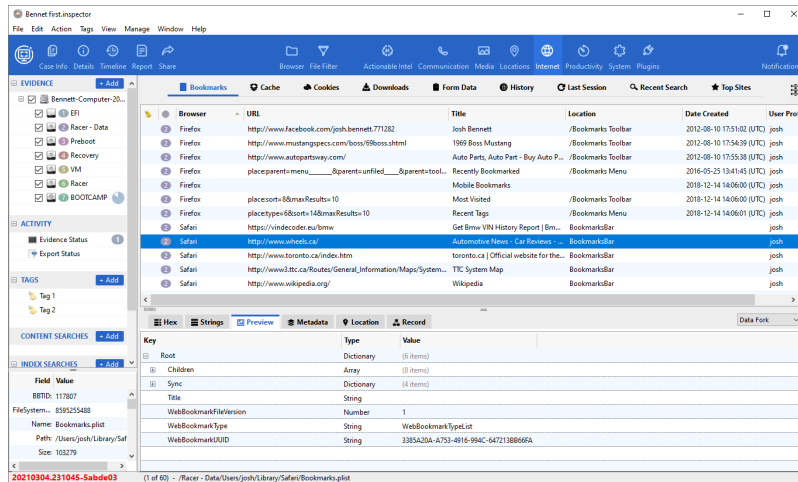
At the top of the Content pane, click **Wi-Fi**. This sub-view shows Wi-Fi networks that the device has joined. Network SSID, BSSID, (signal) Strength, Security (open, WPA2, etc.), Last Joined, and Last Auto Joined information is also shown.

Only networks that the device has joined are listed. Networks that are merely detected and shown as available are not part of this list.

## Internet View

The Internet view shows files associated with Safari, Firefox, Google Chrome, Internet Explorer, and Edge web browsers. This view includes Internet history from Windows and Mac computers as well as iOS and Android devices.

In the Evidence section of the Component list, select a device. On the toolbar, click **Internet**. Internet files appear in the Content pane. By default, Inspector groups Internet log items by browser, so Firefox items will be grouped together, as will Safari and Google Chrome items.



Inspector shows these items in sub-views.

| Item          | Description                                                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bookmarks     | A list of saved web addresses                                                                                                                                                                      |
| Cache         | Web documents (HTML pages, images) remembered by the user's browser. Pages that are temporarily cached by a browser load quickly because data does not have to be accessed again from the Internet |
| Cookies       | Files stored by a user's browser from a website that has been opened in the browser                                                                                                                |
| Downloads     | List of files downloaded using a browser                                                                                                                                                           |
| Form Data     | Personal data stored in an unencrypted database. May include credit card information, usernames, passwords, etc.                                                                                   |
| History       | A list of websites that have opened in a browser                                                                                                                                                   |
| Last Session  | A list of websites that opened in Safari during the last browser session. Used for crash recovery                                                                                                  |
| Recent Search | A user's most recent searches                                                                                                                                                                      |
| Top Sites     | Safari's visual representation (thumbnail images) of Internet history                                                                                                                              |

These items are often stored as either a .plist file, within an SQLite database file, or *INDEX.DAT* files (in the case of Internet Explorer).

In the Content pane, select an Internet cache item. At the top of the File Content view, click **Preview**. Cache file contents (including cached pictures when available) display.

**Note:** A forensic image acquisition must be performed on an iOS device to examine the device's Internet cache. If a logical data acquisition is performed, only history, bookmarks and the iOS device's suspended-state data may be accessible. The suspended-state data on an iOS device represents the open web screens in Safari on the iOS device. Also, as of iOS 8.3 Apple has discontinued access to app data containers. User preferences, documents, and other primary data can still be acquired in an iTunes backup, but certain transitory data and caches, including web content and media, is not included in backups and thus is no longer available for examination.

Inspector includes analysis support for these browsers.

| Browser                                    | Supported Type                           |
|--------------------------------------------|------------------------------------------|
| Microsoft Internet Explorer v5 - 9.0       | Client UrlCache MMF Ver 5.2              |
| Microsoft Internet Explorer v10, v11, Edge | Extensible Storage Engine (ESE) database |
| Mozilla Firefox v3 - 70                    | SQLite and Cache Map                     |
| Google Chrome v0.2 -78                     | History and Cache                        |
| Apple Safari Mac OS X v1 - 13.0.3          | Binary/XML History and Cache.db          |

## Productivity View

On the toolbar, click **Productivity**. The Productivity view has two sub-views, Calendar and Notes.

### Calendar Sub-view

At the top of the Content pane, click **Calendar** see calendar events and notes from the Calendar application (for macOS and iOS).

Calendar events are displayed with time zone information. If Floating appears in the Time Zone column, the event is set to adjust the time zone automatically according to the devices clock. Notes associated with calendar events are displayed. They may contain contact names, phone numbers, directions, and so forth.

Deleted calendar items appear in *red italic* font.

## Notes Sub-view

At the top of the Content pane, click **Notes** to see notes stored with the Notes application (for macOS and iOS) and the Stickies application.

The Notes app on macOS and iOS has two storage options. Depending on the version of macOS and iOS, notes may be stored in *notes.sqlite* or *NoteStore.sqlite*. Notes can be stored locally on the device or in iCloud. iCloud notes are synced across devices that use the same iCloud account.

The notes from the Stickies app are stored in *~/Library/StickiesDatabase*.

Inspector parses notes from *notes.sqlite*, *NoteStore.sqlite*, and *StickiesDatabase*. Data is parsed into these columns in the Content pane.

- Date Created
- Date Modified
- Title
- Summary
- Account
- Source/Folder

The Source/Folder column indicates where the note came from. Notes can be synced using Google and Microsoft Exchange. These are shown along with iCloud notes and locally stored notes. For data stored in Stickies, the Account and Source/Folder fields are empty.

Parsed data can be sorted using any of the Content pane columns. When a note is selected from the list in Content pane, the note text appears in the Note Body section of pane for notes stored in *notes.sqlite* and *NoteStore.sqlite*.

If a note has multiple attachments, you can see those attachments in the Note Body section. You can see the content of attachments by clicking on an attachment and viewing it in the Preview tab. You can see the content in the other tabs as well.

When you tag a note, any attachments that are part of the tagged note are automatically included.

Inspector displays deleted Notes records in *red italic* font.

## System View

With an item selected in the Evidence list, only the sub-views appropriate for the type of item are available.

This chapter provides these topics about these sub-views in the System view in Inspector.

- [Registry](#)
- [Spotlight](#)
- [Dictionary](#)
- [Applications](#)
- [System Logs](#)
- [Memory](#)

## Registry

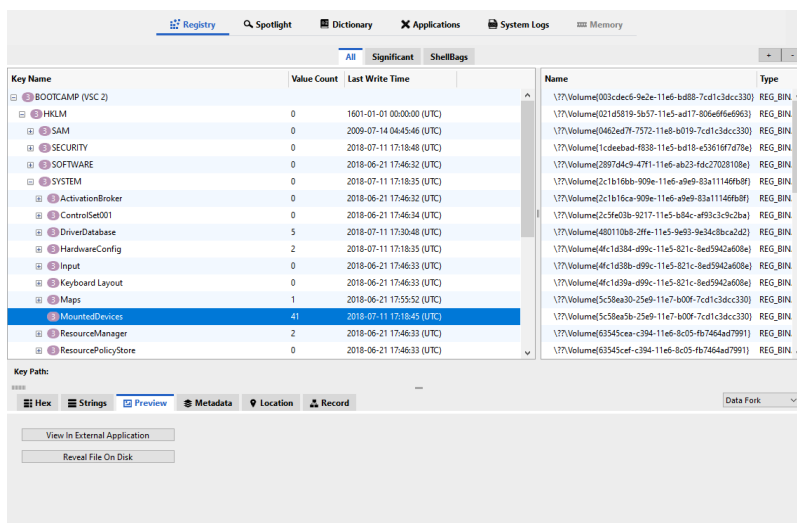
The Windows Registry page on *Wikipedia*, [https://en.wikipedia.org/wiki/Windows\\_Registry](https://en.wikipedia.org/wiki/Windows_Registry), provides this information about the Windows Registry (as of April 2021).

*The Windows Registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry. The kernel, device drivers, services, Security Accounts Manager, and user interfaces can all use the registry. The registry also allows access to counters for profiling system performance....*

*There are seven predefined root keys, traditionally named according to their constant handles defined in the Win32 API, or by synonymous abbreviations (depending on applications):*

- *HKEY\_CLASSES\_ROOT (HKCR)*
- *HKEY\_LOCAL\_MACHINE (HKLM)*
- *HKEY\_CURRENT\_CONFIG (HKCC)*
- *HKEY\_USERS (HKU)*
- *HKEY\_CURRENT\_USER (HKCU)*
- *HKEY\_PERFORMANCE\_DATA (only in Windows NT, but invisible in the Windows Registry Editor)*
- *HKEY\_DYN\_DATA (only in Windows 9x, and visible in the Windows Registry Editor)*

To see Windows Registry files in Inspector, first select a Windows device in the Evidence section of the Component list. On the toolbar, click **System > Registry**. Inspector shows Registry keys hierarchically by root-level hives/files.



Windows Registry files often contain important forensic evidence such as usernames and passwords, Internet browser artifacts, recently accessed files, installed applications, uninstalled applications, etc. They have two basic elements: keys and values. Keys are container objects that are similar to folders, and values are non-container objects that are similar to files.

The Registry is full of places to look for important data. One of the simplest ways to locate the data is by searching the Registry for a value or a key or both. The Find option allows you to quickly search keys, values, and data. It is possible to keep searching for the next occurrence of a specified text string.

Use the Find keystrokes for your computer's operating system to open the Registry Find dialog window. This searches through every Registry item beginning with the currently selected Registry key.

By default, the Registry sub-view displays the most common root keys and sub-keys. You can view additional Registry keys, including those that contain backup Registry files, Registry logs, or incremental updates that may or may not contain relevant data.

**Note:** Some Windows Registry data is volatile and may not be retained after a computer is shut down. Keep this in mind if you encounter a live dual-boot Mac computer.

To see all Registry items, at the top of the Content pane, click **All**. Inspector shows every Registry file on the system. All files except the key files appear under the Other root key.

**Note:** If the File Types process has not yet been run on the selected device, it is possible that some Registry items may not be shown in the Registry sub-view. Some Registry files exist in common, known locations, and these files are parsed automatically by Inspector during the optimization stage of processing. Additional Registry files may exist in other locations throughout the system. These Registry files are discovered during File Types processing, which examines each file and determines its file type. If Inspector discovers additional Registry files during File



Types processing, it parses them and displays them in the Registry sub-view. Select **Evidence Status** in the Component List and ensure that a green checkmark appears in the File Types column for the device, denoting that File Types has been run. You may also click **Run** in the File Types column for the device. Select the device in the Component list and return to the Registry sub-view to see the complete list of Registry items.

You can also see an abridged Registry key set. At the top of the Content pane, click **Significant**.

Unlike the All tab, the Significant tab shows only keys that most often contain important forensic evidence, such as usernames, passwords, and browser history. Hover over a Registry item in this view, and a tool tip appears with information about the item.

|                                                                             |   |                           |                           |
|-----------------------------------------------------------------------------|---|---------------------------|---------------------------|
| ▼ 9 NetworkCards                                                            |   |                           | 2015-06-12 11:51:21 (UTC) |
| Maintains a list of network adapters; the list is held in numbered subkeys. |   |                           |                           |
| ▼ 9 0x11555555                                                              |   |                           |                           |
| 9 159439476E3A00F9FAE49DD6C1A78F2F6288A5B9                                  | 5 | 2015-06-12 11:52:32 (UTC) |                           |
| 9 1A9F109A8ACEE4CA1F898708DBB0FBA6EF0587FC                                  | 5 | 2015-06-12 11:51:39 (UTC) |                           |
| 9 1FCF3C93707C46D648F0B00E216A55E96DEB5A17                                  | 5 | 2015-06-12 11:54:38 (UTC) |                           |
| 9 277F15E06E6EB458048F41BCB8FB843B3241E95                                   | 5 | 2015-06-12 11:52:11 (UTC) |                           |
| 9 3D6DDDC8F8961C8C866F6660579A59B5B6CFA281F                                 | 5 | 2015-06-12 11:51:33 (UTC) |                           |
| 9 551732BB0872DA97E26385C221B172A5BD4DE93C                                  | 5 | 2015-06-12 11:52:12 (UTC) |                           |
| 9 57AFA39B22ADECA4E383572E9331167546EB3C9C7                                 | 5 | 2015-06-12 11:52:32 (UTC) |                           |
| 9 5BEF08C10896D86DC13394FFA75874564B700368                                  | 5 | 2015-06-12 11:52:32 (UTC) |                           |
| 9 742CB1BDA52EA9F1BBE482DA6DAA17944652B476                                  | 5 | 2015-06-12 11:52:11 (UTC) |                           |
| 9 75E64992A03EC5E73D33586790CC506561DCC5DB                                  | 5 | 2015-06-12 11:51:34 (UTC) |                           |
| 9 969EFE1D5E95B01D3C42B9D0363FA64AF9E336E7                                  | 5 | 2015-06-12 11:51:58 (UTC) |                           |
| 9 9EBC96DD99F2C854D540FBF6A16A557BADD8C228                                  | 5 | 2015-06-12 11:51:59 (UTC) |                           |
| 9 A5E73046BA905B7B0235AB40FA98A4E3AB96E00E                                  | 5 | 2015-06-12 11:51:23 (UTC) |                           |
| 9 ABCCA6C3F97A148D7C69114CB55DFA9D46053BEA                                  | 5 | 2015-06-12 11:50:50 (UTC) |                           |

You can add items to the Significant view. Click your choice of **Default**, **All**, or **Significant** sub-views. Select an item in the list and click **+ (add)** in the top right next to Add/Remove From Significant Items. Navigate to the Significant view if not already there. The added item is shown at the bottom of the list of Registry items. To remove an item from the list, select it and click **- (remove)** in the top right next to Add/Remove From Significant Items. Preset Registry items cannot be removed from the Significant list.

## Shellbags

Shellbags are a type of Windows Registry key that may provide useful information, including a user's display preferences for a folder, timestamps for when a folder was first visited and last updated, and sometimes information about deleted folders.

In the toolbar, click **System > Registry > ShellBags**.

| All Significant ShellBags       |                       |                 |      |                           | Field Value                                 |
|---------------------------------|-----------------------|-----------------|------|---------------------------|---------------------------------------------|
| Name                            | Type                  | Bag Path        | Slot | Created Date              |                                             |
| BOOTCAMP (VSC 1)                |                       |                 |      |                           | Path Desktop\My Computer (This PC)\Unkno... |
| BOOTCAMP (Active)               |                       |                 |      |                           | Last Write Date 2018-06-21 17:55:36 (UTC)   |
| josh                            |                       |                 |      |                           | Type ID 31                                  |
| ShellBagsMRU                    |                       |                 |      |                           | Extension Blocks                            |
| Desktop                         |                       |                 |      |                           | Signature 0x00000000                        |
| Control Panel (Category View)   | System Folder         | BagMRU\0        | 1    |                           | Size 80                                     |
| My Computer (This PC)           | System Folder         | BagMRU\1        | 13   |                           | Version Offset 22                           |
| D:\                             | Volume                | BagMRU\1\0      | 6    |                           | Version 9                                   |
| Unknown CLSID: f046385-37ec...  | Root Folder: GUID     | BagMRU\1\1      | 8    |                           | OS Version 8.1                              |
| Unknown CLSID: 088a3905-0323... | Root Folder: GUID     | BagMRU\1\10     | 171  |                           | System Identifier ZE                        |
| Unknown CLSID: 939ce936-01d2... | Root Folder: GUID     | BagMRU\1\11     | 173  |                           | MFT Entry Number 3325                       |
| C:\                             | Volume                | BagMRU\1\12     | 32   |                           | MFT Sequence Number 7                       |
| Nexus 5                         | Root Folder: MTP D... | BagMRU\1\13     | 43   |                           | File System NTFS                            |
| Nexus 5                         | Root Folder: MTP D... | BagMRU\1\14     | 63   |                           | Long Name Uploads                           |
| Nexus 5                         | Root Folder: MTP D... | BagMRU\1\15     | 71   |                           | Localized Name Upload                       |
| E:\                             | Volume                | BagMRU\1\16     | 115  |                           | Date Created 2017-03-30 15:54:12 (UTC)      |
| G:\                             | Volume                | BagMRU\1\17     | 119  |                           | Date Accessed 2017-04-20 16:52:12 (UTC)     |
| Unknown CLSID: 24ad3ad4-a569... | Root Folder: GUID     | BagMRU\1\18     | 169  |                           |                                             |
| Cloud Photos                    | Directory             | BagMRU\1\18\0   | 192  | 2017-03-30 15:54:12 (UTC) |                                             |
| Uploads                         | Directory             | BagMRU\1\18\0\0 | 193  | 2017-03-30 15:54:12 (UTC) |                                             |
| Desktop                         | Root Folder: GUID     | BagMRU\1\19     | 170  |                           |                                             |

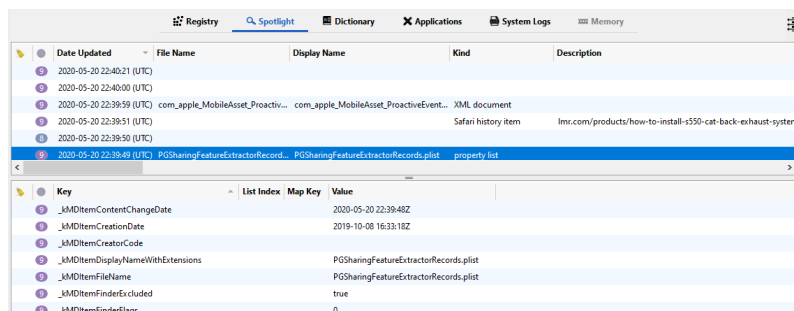
Available shellbag information appears in the left pane. Select one of the folders in the list to see metadata pertaining to the shellbag in the right pane. Metadata is also shown in the File Content view if the Metadata tab is selected.

You can apply Filters to the shellbag data by clicking Show/Hide Filter and applying filter parameters. Individual items or groups of items can also be tagged.

## Spotlight

Spotlight is the Apple's indexing tool built into macOS and iOS. Spotlight data is stored at the root level of any volume that has touched a macOS system. This is known as the System Level store and contains metadata for files on the volume. Spotlight may also store indexed file content in cache text files located at `/.Spotlight-V100/Store-V2/<UUID>/Cache`. For macOS volumes, data is also parsed from the Spotlight stores listed in each user's Library folder. Spotlight files on iOS devices, stored in `/private/var/mobile/Library/Spotlight/CoreSpotLight`, are also parsed.

To see data parsed from Spotlight, in the toolbar click **System > Spotlight**.



| Date Updated              | File Name                          | Display Name                            | Kind                | Description                                                  |
|---------------------------|------------------------------------|-----------------------------------------|---------------------|--------------------------------------------------------------|
| 2020-05-20 22:40:21 (UTC) |                                    |                                         |                     |                                                              |
| 2020-05-20 22:40:00 (UTC) |                                    |                                         |                     |                                                              |
| 2020-05-20 22:39:59 (UTC) | com_apple_MobileAsset_Proactiv...  | com_apple_MobileAsset_ProactiveEvent... | XML document        |                                                              |
| 2020-05-20 22:39:51 (UTC) |                                    |                                         | Safari history item | lms.com/products/how-to-install-4550-cat-back-exhaust-system |
| 2020-05-20 22:39:50 (UTC) |                                    |                                         |                     |                                                              |
| 2020-05-20 22:39:49 (UTC) | PGSharingFeatureExtractorRecord... | PGSharingFeatureExtractorRecords.plist  | property list       |                                                              |

| Key                               | List Index | Map Key | Value                                  |
|-----------------------------------|------------|---------|----------------------------------------|
| _kMDItemContentChangeDate         |            |         | 2020-05-20 22:39:48Z                   |
| _kMDItemCreationDate              |            |         | 2019-10-08 16:33:18Z                   |
| _kMDItemCreatorCode               |            |         |                                        |
| _kMDItemDisplayNameWithExtensions |            |         | PGSharingFeatureExtractorRecords.plist |
| _kMDItemFileName                  |            |         | PGSharingFeatureExtractorRecords.plist |
| _kMDItemFinderExcluded            |            |         | true                                   |
| _kMDItemFinderFlags               |            |         | 0                                      |

The data contained in Spotlight varies depending on the artifact you are viewing. The Content pane is split into two sections. The top portion contains columns of data with information parsed directly from the database and data parsed from the Spotlight metadata keys. The first column, Date Updated, and the columns all the way to the right (Item ID, OID, Parent OID, and Cache File) correspond to data contained in the Spotlight database. Between these columns is the information parsed from the Spotlight metadata keys. For example, the Spotlight metadata key `_kMDItemFileName` is displayed in the File Name column. The very last column, Source, contains the name of the Spotlight database the information was parsed from. The bottom portion of the Content pane lists all of the Spotlight metadata values parsed for each entry. Since Spotlight metadata varies, not all metadata items listed at the bottom will have a corresponding column at the top of the Content pane.

- Account Handles
- Account Identifiers
- Account Type
- Bundle ID
- Cache File
- Content Creation Date
- Content Modification Date
- Content Type
- Content URL
- Creation Date
- Date Added
- Date Updated
- Description
- Display Name
- External ID
- File Name
- Item ID
- Kind
- Last Used Date
- OID
- Parent OID
- Source
- Storage Size
- Use Count

The screenshot shows the Spotlight search interface in macOS. The top navigation bar includes tabs for Registry, Spotlight (selected), Dictionary, Applications, System Logs, and Memory. The main area displays a list of search results with columns for Date Updated, File Name, Display Name, Kind, Description, Use Count, Last Used Date, and Content Creation Date. A context menu is open over the file 'BMW\_Info.indd', showing various actions. The 'Reveal' option is highlighted, and a sub-menu is visible, showing options like 'File On Disk', 'File in File Browser', 'File in Disk View', 'Reveal Date in Timeline', 'Item in Native View', and 'Reveal Cache File in File Browser'.

Spotlight is also known to index content such as calendar entries, Evernotes, email, and reminders. Snippets of content from these sources can be found in the parsed Spotlight data.

| Date Updated              | File Name                 | Display Name              | Kind              | Description | Use Count | Last Used Date | Creation Date             | Content Creation Date |
|---------------------------|---------------------------|---------------------------|-------------------|-------------|-----------|----------------|---------------------------|-----------------------|
| 2020-05-19 21:23:18 (UTC) | text.txt                  | text.txt                  | Document          |             |           |                | 2019-09-25 01:11:00 (UTC) | 2019-09-25 01:11:00   |
| 2020-05-19 21:23:21 (UTC) | text.rim                  | text.rim                  | Document          |             |           |                | 2019-09-04 02:39:00 (UTC) | 2019-09-04 02:39:00   |
| 2020-05-19 21:23:18 (UTC) | Text@2x.png               | Text@2x.png               | PNG image         |             |           |                | 2019-09-17 04:43:50 (UTC) | 2019-09-17 04:43:50   |
| 2020-04-27 22:16:20 (UTC) | text.plist                | text.plist                | NSStringBoardType |             |           |                | 2019-12-07 17:12:04 (UTC) | 2019-12-07 17:12:04   |
| 2020-05-19 21:23:17 (UTC) | text_align-H_center_N.off | text_align-H_center_N.off | TTF image         |             |           |                | 2019-08-25 02:24:08 (UTC) | 2019-08-25 02:24:08   |
| 2020-05-19 21:23:17 (UTC) | text_align-H_center_S.off | text_align-H_center_S.off | TTF image         |             |           |                | 2019-08-25 02:24:08 (UTC) | 2019-08-25 02:24:08   |

| Key                                    | List Index | Map Key | Value                                                                                                          |
|----------------------------------------|------------|---------|----------------------------------------------------------------------------------------------------------------|
| _kMDItemFinderLabel                    |            |         | 0                                                                                                              |
| _kMDItemFromImporter                   |            |         | true                                                                                                           |
| _kMDItemGroupID                        |            |         | 14                                                                                                             |
| _kMDItemInterestingDate                |            |         | 2019-12-07 17:12:04Z                                                                                           |
| _kMDItemExtensionHidden                |            |         | false                                                                                                          |
| _kMDItemOwnerGroupID                   |            |         | 20                                                                                                             |
| _kMDItemOwnerUserID                    |            |         | 501                                                                                                            |
| _kMDItemSnippet                        |            |         | Missed your birthday, sorry. Hope it was wild! Guess maybe I'll see you next month with the boys. Drinks on me |
| _kMDItemStorageSize                    |            |         | 378                                                                                                            |
| _kMDItemTextContentIndexExists         |            |         | true                                                                                                           |
| _kMDItemTextEncodingInt                |            |         | 134217984                                                                                                      |
| _kMDItemTypeCode                       |            |         |                                                                                                                |
| com.apple.mail.dataReceived            |            |         | 2019-11-23 22:38:34Z                                                                                           |
| com.apple.mail.dataSent                |            |         | 2019-11-23 22:38:31Z                                                                                           |
| com.apple.mail.isRemoteAttachment      |            |         | false                                                                                                          |
| com.apple.mail.transaction             |            |         | 2626                                                                                                           |
| kMDItemAccountIdentifier               |            |         | 96936521-EAC7-4961-9648-21876308743F                                                                           |
| kMDItemContentCreationDate_Ranking     |            |         | 2019-12-07 17:12:04Z                                                                                           |
| kMDItemContentModificationDate_Ranking |            |         | 2019-12-07 17:12:04Z                                                                                           |
| kMDItemContentModificationDate_Ranking |            |         | 2019-12-07 17:12:04Z                                                                                           |

## Tagging Spotlight Data

If a Spotlight data entry is tagged in the top portion of the Content pane, all Spotlight metadata values parsed shown in the lower portion of the Content pane are automatically tagged.

| Date Updated              | File Name                  | Display Name               | Kind              | Description | Use Count | Last Used Date | Creation Date             | Content Creation Date |
|---------------------------|----------------------------|----------------------------|-------------------|-------------|-----------|----------------|---------------------------|-----------------------|
| 2020-05-19 21:23:18 (UTC) | Text@2x.png                | Text@2x.png                | PNG image         |             |           |                | 2019-09-17 04:43:50 (UTC) | 2019-09-17 04:43:50   |
| 2020-04-27 22:16:20 (UTC) | text.plist                 | text.plist                 | NSStringBoardType |             |           |                | 2019-12-07 17:12:04 (UTC) | 2019-12-07 17:12:04   |
| 2020-05-19 21:23:17 (UTC) | text_align-H_center_N.off  | text_align-H_center_N.off  | TTF image         |             |           |                | 2019-08-25 02:24:08 (UTC) | 2019-08-25 02:24:08   |
| 2020-05-19 21:23:17 (UTC) | text_align-H_center_S.off  | text_align-H_center_S.off  | TTF image         |             |           |                | 2019-08-25 02:24:08 (UTC) | 2019-08-25 02:24:08   |
| 2020-05-19 21:23:17 (UTC) | text_align-H_justify_N.off | text_align-H_justify_N.off | TTF image         |             |           |                | 2019-08-25 02:24:08 (UTC) | 2019-08-25 02:24:08   |
| 2020-05-19 21:23:17 (UTC) | text_align-H_justify_S.off | text_align-H_justify_S.off | TTF image         |             |           |                | 2019-08-25 02:24:08 (UTC) | 2019-08-25 02:24:08   |

| Key                               | List Index | Map Key | Value                                                                                                          |
|-----------------------------------|------------|---------|----------------------------------------------------------------------------------------------------------------|
| _kMDItemBundleID                  |            |         | com.apple.mail                                                                                                 |
| _kMDItemContentChangeDate         |            |         | 2019-12-07 17:12:04Z                                                                                           |
| _kMDItemCreationDate              |            |         | 2019-12-07 17:12:04Z                                                                                           |
| _kMDItemCreatorCode               |            |         |                                                                                                                |
| _kMDItemDisplayNameWithExtensions |            |         | text.plist                                                                                                     |
| _kMDItemDomainIdentifier          |            |         | 96936521-EAC7-4961-9648-21876308743F.3                                                                         |
| _kMDItemExpirationDate            |            |         | 2247-05-05 01:16:18.871345192Z                                                                                 |
| _kMDItemExternalID                |            |         | attachment:13                                                                                                  |
| _kMDItemFileName                  |            |         | text.plist                                                                                                     |
| _kMDItemFinderFlags               |            |         | 9                                                                                                              |
| _kMDItemFinderLabel               |            |         | 0                                                                                                              |
| _kMDItemFromImporter              |            |         | true                                                                                                           |
| _kMDItemGroupID                   |            |         | 14                                                                                                             |
| _kMDItemInterestingDate           |            |         | 2019-12-07 17:12:04Z                                                                                           |
| _kMDItemExtensionHidden           |            |         | false                                                                                                          |
| _kMDItemOwnerGroupID              |            |         | 20                                                                                                             |
| _kMDItemOwnerUserID               |            |         | 501                                                                                                            |
| _kMDItemSnippet                   |            |         | Missed your birthday, sorry. Hope it was wild! Guess maybe I'll see you next month with the boys. Drinks on me |
| _kMDItemStorageSize               |            |         | 378                                                                                                            |
| _kMDItemTextContentIndexExists    |            |         | true                                                                                                           |
| _kMDItemTextEncodingInt           |            |         | 134217984                                                                                                      |

In the Report, the information parsed in the upper portion of the Content pane is shown together, followed by a separate table for each Spotlight metadata values parsed for that entry.

One entry tagged in the top portion of the Content pane can result in numerous tagged items since all parsed Spotlight metadata values shown in the lower portion of the Content pane are automatically tagged.

Unfortunately, the reverse is not so easy. If an entry tagged from the top portion of the Content pane is removed, the corresponding parsed metadata values in the lower portion of the Content pane are not removed from the tag. To remove all of the tagged data, select all of the tagged entries in the lower portion of the Content pane, open the context menu, and then click **Remove Apple Spotlight From Tag Group**.

## Dictionary

On the toolbar, click **System > Dictionary**. The predictive text data from the dynamic dictionary database is displayed. This database file stores user-entered text strings typed on the keyboard. This may include usernames, web passwords and other login credentials, website URLs, and text from SMS and email messages. Depending on the device and operating system, these text strings may be stored in the chronological order they were typed.

If a user stored passwords in an unsecured application, such as the Notes application, or accidentally typed a password into the wrong field on a login form, the text containing the password may be stored in this file. The iOS operating system does not store passwords that a user typed into a designated password text field.

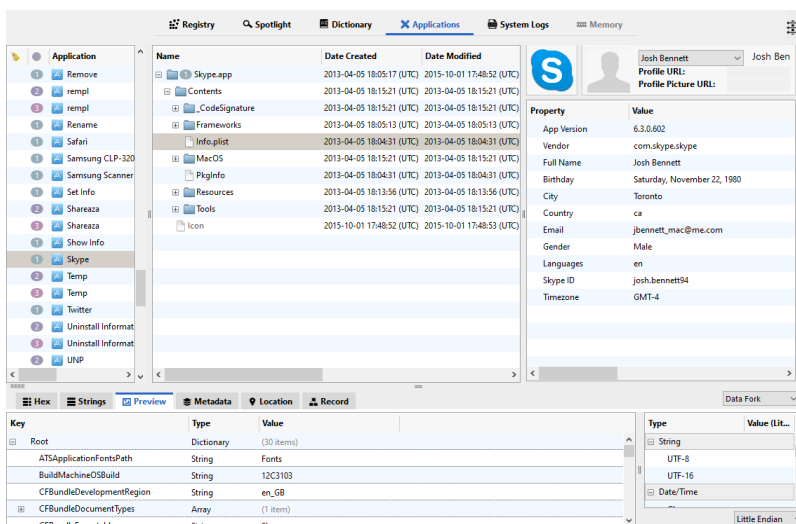
The text in this database file can be used to potentially aid in cracking passwords on the device. In the Content pane, select one or more dynamic text entries. Open the context menu and select **Export as CSV**. Select a file export location and click **Export**. A text file containing all the selected words is saved.

## Applications

There are about 900,000 applications available from the Apple App Store. Inspector provides a uniform way to view these applications and application bundle contents during a forensic examination.

On the toolbar, click **System > Applications**. The Applications sub-view shows a comprehensive list of user-installed third-party applications and their icons. Select an application from the list at left. The middle pane shows the application bundle contents, and certain application data is parsed and shown in the right pane. The data in the right pane may include a username, email address, app version, and last login date.

In the middle pane, when you select a file associated with an application, such as a PDF, image file, or database, the file appears in the File Content view. To examine the files using different views, scroll through the Hex, Strings, Preview, Metadata, and Quick Look (Mac only) views at the top of the File Content view. Select a column heading to sort specific application files by Name, Date Created, Date Modified, Date Accessed, Date Added, or Size.



Applications like Facebook and Skype store contact and conversation data in database files.

**Note:** iOS Backup folders contain mostly user-specific data. Therefore, iOS Backup folders do not store all application data. Purchase date, release date, and the Apple ID used to purchase the App cannot be seen during an analysis of the iOS Backup folder. Custom application icons are not contained in a backup folder either; a generic icon is shown instead.

If third-party application information is important, be sure to perform a forensic image acquisition (using third party software) or a logical data acquisition when adding iOS data to a case.

## System Logs

In System View, System Logs offers views of File System Logs and Unified Logs.

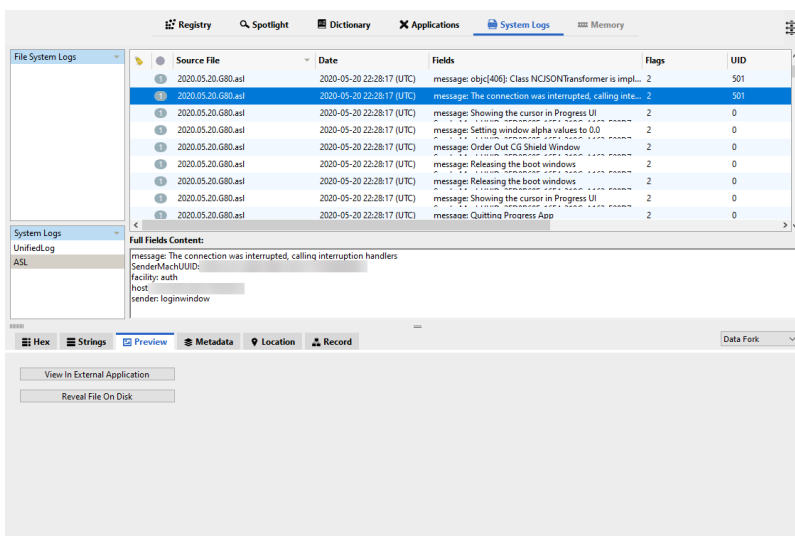
### File System Logs

Inspector parses system logs from both Windows and macOS computers. The File System Journal Analysis processing option parses the *\$Logfile*, containing disk activity, and *\$USNJRNL*, the change journal file, on Windows computers and *.fsevents* on macOS. The OS Event / Security Logs processing option parses Windows event logs (EVT and EVT\_X), macOS Apple System Logs (ASL), and Unified Logs. For more information, see [Adding a Disk Image](#).

Once these processing options are run, you can see the results in the System Logs sub-view of the System view.

On the toolbar, click **System > System Logs**. In the list to the lower left, click **System Logs**. The Content pane is divided into sections. On the left side, the upper pane lists parsed File System Logs. The lower pane lists parsed System Logs. The right side of the Content pane shows the item selected on the left.

**Note:** Event IDs in *.fsevents* logs may not reflect the actual order in which events took place. This means you cannot make assumptions about events based on their event IDs and the source file's date and time. This information cannot be relied upon to prove a chronological order.



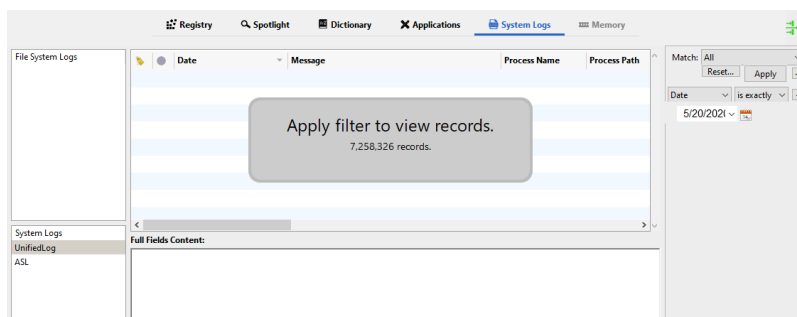
## Unified Logs

As of macOS 10.12, Apple introduced the unified logs format. This was done to have a common log format across all Apple operating systems, including macOS, iOS, watchOS, and tvOS. Unified logs are parsed with the OS Event / Security Logs initial processing option or Events/Logs from Evidence Status.

The amount of data stored in Unified Logs is massive. During times of intense activity, 10,000 records can be added to the logs in a minute. This can result in millions of records in Unified Logs. Loading millions of records into Inspector and manually reviewing them could take a significant amount of time. Therefore, you must filter Unified Log records for data of interest.

To see unified logs, on the toolbar click **System > System Logs**. Then, in the list to the left, click **UnifiedLog**. The Content pane is divided into sections. On the left side, the upper pane lists parsed File System Logs. The lower pane lists parsed unified logs.

Unified Logs do not load automatically. Instead, Inspector presents a message showing the total number of records and requiring you to apply a filter to view them. The filter pane automatically appears on the right side of the Content Pane.



Log records can be filtered by these options, parsed for each record.

- Any (any string)
- Date
- Type
- UID
- PID
- Process Name
- Process Path
- Sender Name
- Sender path
- Message
- Offset
- Subsystem
- Category
- Signpost Name
- Signpost Info

Filters can be created for records during a timeframe of investigative interest. Dates in Unified Logs records are stored in the Inspector database down to nanoseconds, and records appear in microsecond precision. Sorting with the Date column shows the records in order by timestamps. The Date column is the only sortable column for Unified Logs.

Unified Logs may contain data regarding time machine backups, time zone changes, external media mount and unmount, or connected printer.

Due to the volume of Unified Log events, they are not included in the smart index. Any USB device information parsed from Unified Logs is also added to the Actionable Intel view.

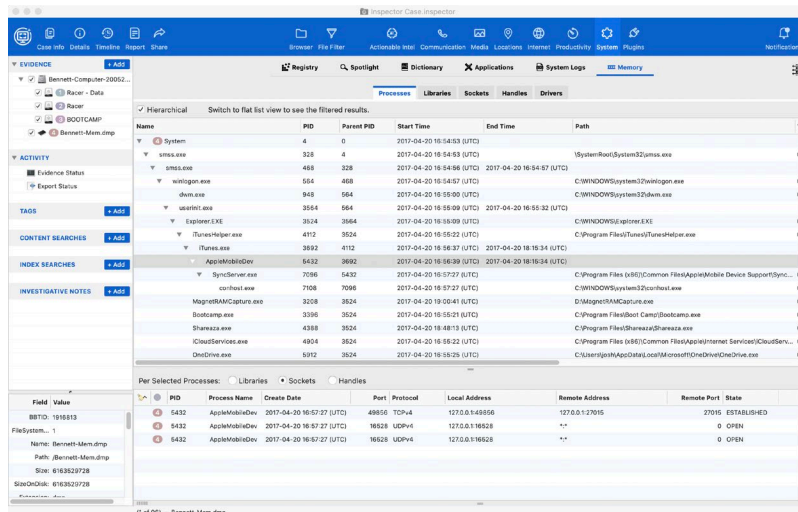


## Memory

For the contents of a memory file to be parsed and displayed, advanced processing options must first be run. For more information, see [Adding a Memory File](#).

Once advanced processing has been run on the memory file, the contents can be viewed in the Memory sub-view.

On the toolbar, click **System > Memory**.



The Memory sub-view provides these deeper views for analyzing memory file artifacts.

- Processes
- Libraries
- Sockets
- Handles
- Drivers

Select one or more processes from the upper pane in the Processes sub-view, and any libraries, sockets, and handles associated with the selected processes (like having the same PID) appear in the lower pane. To see these artifacts in those views, click **Libraries**, **Sockets**, or **Handles**.

**Note:** The information in the Description column for libraries is taken from this source: <http://www.softwaretipsandtricks.com/dll/>.



## Actionable Intel View

The Actionable Intel view in Inspector allows you to see various types of data points that can mostly be attributed to a user's actions. The Actionable Intel view provides a tree style menu with sub-view menus.

This chapter provides these topics about the Actionable Intel view.

- [Device Backups](#)
- [Device Connections](#)
- [Account Usage](#)
- [Downloads](#)
- [File Knowledge](#)
- [Passwords](#)
- [Program Execution](#)
- [Search](#)
- [Activity Correlation](#)

## Device Backups

In Actionable Intel, Device Backups offers a view of iOS backup folders contained on the selected partition, along with the model, phone number, last backup date, OS version, serial number, UDID and IMEI.

To see device backups, on the toolbar click **Actionable Intel**, then in the menu to the left, click **Device Backups**.

| Name                  | Model                                       | Phone Number      | Last Backup Date          | OS Version | Serial Number | UDID      |
|-----------------------|---------------------------------------------|-------------------|---------------------------|------------|---------------|-----------|
| Josh Bennett's iPad 2 | iPad 2                                      |                   | 2015-02-08 23:01:03 (UTC) | 8.1.3      | DUXFK8CYDFFHW | 25ccc0bd1 |
| The6                  | iPhone 8 (Model A1863, A1905, A1906, A1907) | +1 (240) 494-6399 | 2020-01-10 20:41:29 (UTC) | 13.3       | C8KVLLUXJCN   | 72bb6c84f |

## Exporting iOS Backups

Select a backup, then click **File > Add Selected**.

A message appears to advise that the backup item must be exported and reimported before it is available for analysis. Click **Continue**.

In the Activity section of the Component list, click **Export Status** to see the backup folder export progress. When the export completes, the Add Evidence window appears, where you can import the iOS backup into the case.

Mark the checkbox for the iOS backup to be imported. If the backup is encrypted, a lock icon appears next to the backup name. Click on the lock icon (next to the backup name in the middle column), and a dialog box opens, prompting for the password that was in effect when the backup was made.



Enter the password and click **Confirm Password**. Without the backup password, only ancillary data is available for collection, such as media and some third-party application data.

**Note:** The encrypted backup password is not the device's PIN code. The encrypted backup password is a password that a user has set in iTunes when backing up an iOS device to a computer.

## Importing iOS Backups

In the middle portion of the Add Evidence view, you can edit the Evidence ID field with an alphanumeric evidence ID for the iOS backup folder.

Choose the ingestion options and click **Start** to begin the import.

**Note:** Because an iOS backup folder import contains only logical data, the backup folder does not contain unallocated space the way a bit-by-bit forensic image of the iOS devices would.

In the Activity section of the Component list, click **Evidence Status** to see the progress of importing the backup folder. When the import completes, the backup folder, along with the backup folder name and device-appropriate icon, appear in the Evidence section of the Component list.

For more information, see [Managing Case Evidence](#).

## Device Connections

In Actionable Intel, Device Connections offers a view of all devices previously connected to the source computer. Among other things, you can see the connected device type, serial number, last connected timestamp, and the number of times the device was connected (for iOS devices).

To see previously connected devices, on the toolbar click **Actionable Intel**, then in the menu on the left, click **Device Connections**.

| Product Name                       | Serial Number            | Last Connected Date       | User Name | Use Count |
|------------------------------------|--------------------------|---------------------------|-----------|-----------|
|                                    | 08606ED40B6B06118181BA4  | 2020-05-01 19:08:19 (UTC) | Unknown   | 1         |
|                                    | 001CC0C6117C8C8183190248 | 2020-04-29 17:37:58 (UTC) | Unknown   | 1         |
|                                    | 001CC0C6117C8C8183190248 | 2020-04-29 17:49:06 (UTC) | Unknown   | 1         |
|                                    | 08606ED40B6B06118181BA4  | 2020-05-19 21:29:22 (UTC) | Unknown   | 1         |
|                                    | 08090952ac225a           | 2020-05-19 21:37:27 (UTC) | Unknown   | 1         |
| CBM2080 / CBM2090 Flash drive c... | 08152300405A7C00         | 2020-04-30 20:25:07 (UTC) | Unknown   | 1         |
| Internal Memory Card Reader        | 000000000310             | 2020-04-27 21:37:39 (UTC) | Unknown   | 1         |
| Internal Memory Card Reader        | 000000000310             | 2020-05-08 20:44:11 (UTC) | Unknown   | 1         |
| Internal Memory Card Reader        | 000000000310             | 2020-05-20 22:28:02 (UTC) | Unknown   | 1         |
| Internal Memory Card Reader        | 000000000310             | 2020-05-01 19:22:27 (UTC) | Unknown   | 1         |
| Internal Memory Card Reader        | 000000000310             | 2020-04-29 17:35:06 (UTC) | Unknown   | 1         |
| Internal Memory Card Reader        | 000000000310             | 2020-05-10 04:43:52 (UTC) | Unknown   | 1         |
| iPad                               | DLXFK6CYDFHW             | 2015-04-14 14:13:46 (UTC) | josh      | 7         |
| iPhone                             | DNPJHMKUDDTQ             | 2016-07-14 16:14:07 (UTC) | Unknown   | 2         |
| iPhone                             | F1FNDWU2G5MG             | 2018-08-20 14:55:06 (UTC) | Unknown   | 20        |
| iPhone                             | FD2VC3L9CM2              | 2020-05-20 22:45:12 (UTC) | Unknown   | 3         |
| iPhone                             | 86935LC53NP              | 2011-07-05 16:54:13 (UTC) | Unknown   | 17        |
| iPhone                             | C6KVKLUXIC6N             | 2020-01-10 20:40:01 (UTC) | Unknown   | 9         |
| iPhone                             | 5K92045KY7K              | 2011-05-20 21:55:50 (UTC) | Unknown   | 2         |
| iPhone                             | DNPJHPHJDTTQ             | 2016-10-26 13:43:54 (UTC) | Unknown   | 22        |
| iPhone                             | FDMQ61LTG5MG             | 2019-02-25 14:45:09 (UTC) | Unknown   | 2         |
| iPhone                             | DNVNGTLG5MC              | 2019-02-26 14:09:39 (UTC) | Unknown   | 6         |
| iPhone                             | DNVNGTLG5MC              | 2019-02-26 14:09:39 (UTC) | josh      | 6         |
| iPhone                             | 8811659CDZZ              | 2012-10-21 14:41:19 (UTC) | josh      | 11        |

**Note:** Timestamps shown in Device Connections parsed from the *system.log* file show the time zone as UNKN to reflect that the time zone is unknown. Since the time zone on *system.log* timestamps is unknown, be aware that the date could be incorrect as a result.

## Account Usage

In Actionable Intel, Account Usage offers views of cellular usage, top contacts, and user accounts.

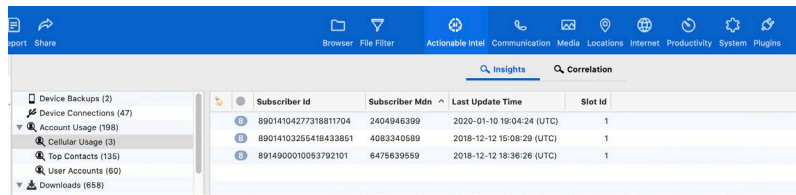
### Cellular Usage

This applies to both iPhone and Android devices; Android depends on device and version.

You can see the parsed contents of this database showing the Subscriber ID, phone number and last update time.

Users of iOS devices can switch SIM cards. Additionally, newer iOS devices are equipped with eSIM capability making it possible for users to store multiple eSIM accounts on a single device. This data is stored in */Library/Databases/CellularUsage.db*.

On the toolbar click **Actionable Intel**, then in the menu on the left, click **Cellular Usage** under Account Usage



## Top Contacts

You can see a list of the device's most frequent contacts along with the message and call counts for each.

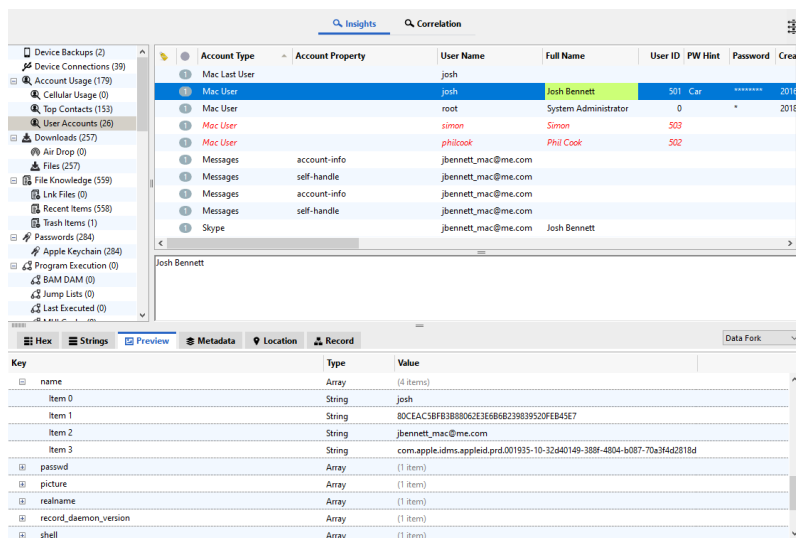
On the toolbar click **Actionable Intel**, then in the menu on the left, click **Top Contacts** under Account Usage.

## User Accounts

You can see user account information for both current and deleted user accounts.

This includes the current user accounts' UID, User Name, Full Name, home folder path, and password hints, along with deleted user accounts' UID, User Name, Full Name, and date deleted information. Timestamps for created, last logon, last password change, last failed logon, and logon count may also show in this view.

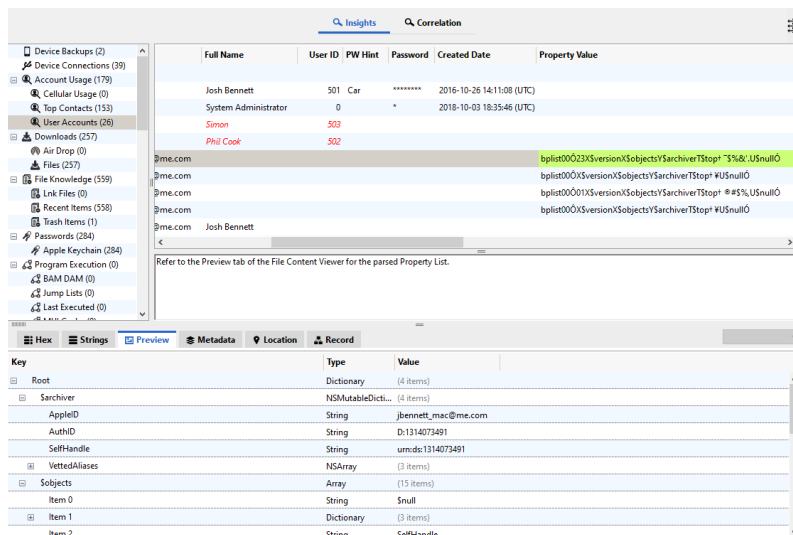
On the toolbar click **Actionable Intel**, then in the menu on the left, click **User Accounts** under Account Usage.



For User Account entries stored in binary plists, you can select an entry in one column (highlighted green). Only data in the highlighted data appears in the lower portion of the Content pane.

In macOS, account information is also parsed from databases stored in `~/Library/Accounts`, providing information about the user name and account type. Databases in `~/Library/Accounts` store information about the user's other accounts including iCloud, social media, email, and calendars. This data is parsed and displayed with operating system user accounts. Entries stored in the Account databases often contain a binary property list in the database entry.

To see the data stored in the binary plist, select an entry in the **Property Value** column. The data is highlighted in green. The Preview tab in the File Content view shows the parsed property list.



## Downloads

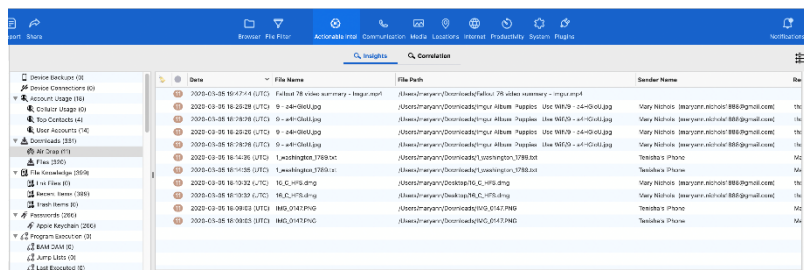
In Actionable Intel, Downloads offers views of AirDrop and Files.

## AirDrop

AirDrop is a macOS and iOS feature to transfer files to other nearby Apple devices. Artifacts from AirDrop on macOS are stored in multiple locations including Unified Logs and Spotlight. Inspector parses AirDrop artifacts from Spotlight, which contains more complete information.

To see AirDrop artifacts, on the toolbar click **Actionable Intel**, then in the menu on the left, click **Air Drop** under Downloads.

For more information, see these topics provided by Apple.



- <https://support.apple.com/en-us/HT204144>
- <https://support.apple.com/en-us/HT203106>

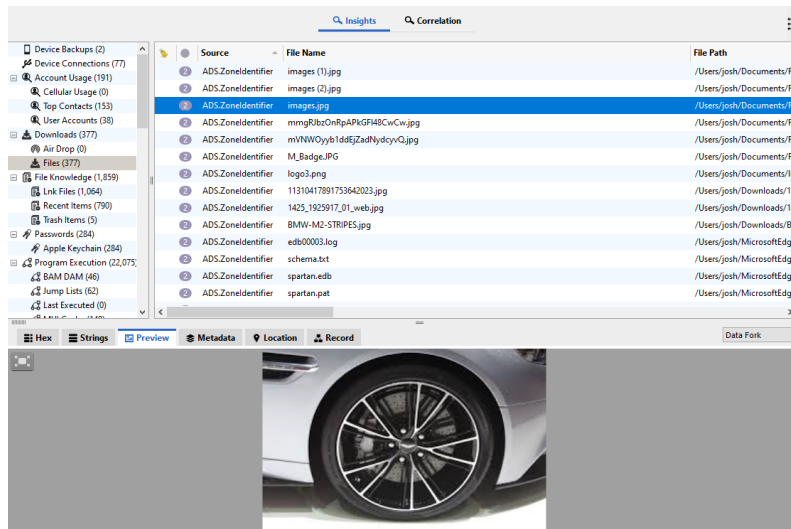
## Files

Files shows information about recent file downloads. Some or all of this information may be shown.

- source (such as Internet Explorer, Chrome, Safari, or Firefox)
- file name
- file path
- timestamp
- sender name
- sender address
- title

Web browsers have built-in download managers that keep a history of every file downloaded by a user. These browser artifacts can provide excellent information about what sites a user has been visiting and what files were downloaded. In addition to browser downloads, Files also includes artifacts from *Zone.Identifier* files in Windows and quarantine files in macOS.

To see information about recent file downloads, on the toolbar click **Actionable Intel**, then in the menu on the left, click **Files** under Downloads.



## File Knowledge

In Actionable Intel, File Knowledge offers views of Link Files, Recent Items, and Trash Items.

### Link Files

On Windows systems, link (.lnk) files may be created by the operating system during routine operation or be deliberately created by a user. To see Windows link files, on the toolbar click **Actionable Intel**. In the menu on the left, click **Link Files** under File Knowledge. Metadata for selected link files includes link attribute, link target information, and target system information. To see this metadata in the File Content view, click **Preview**. In this view, you can tag individual rows for reporting purposes.

| File Name                                                                                           | Link Target                                                                                         |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| JBMemDump.dmp.lnk                                                                                   | JBMemDump.dmp                                                                                       |
| JBMem.dmp.lnk                                                                                       | JBMem.dmp                                                                                           |
| JB.dmp.lnk                                                                                          | JB.dmp                                                                                              |
| 2017-porsche-boxster-facelift-revealed-in-latest-spyshots-has-cayenne-like-tailight-graphics_26.lnk | 2017-porsche-boxster-facelift-revealed-in-latest-spyshots-has-cayenne-like-tailight-graphics_18.lnk |
| 2017-porsche-boxster-facelift-revealed-in-latest-spyshots-has-cayenne-like-tailight-graphics_18.lnk | 2017-porsche-boxster-facelift-revealed-in-latest-spyshots-has-cayenne-like-tailight-graphics_18.lnk |
| 2016-bmw-m2-04-1.lnk                                                                                | 2016-bmw-m2-04-1.jpg                                                                                |
| 2016-bmw-m2-01-1.lnk                                                                                | 2016-bmw-m2-01-1.jpg                                                                                |
| 11310417891753642023.lnk                                                                            | 11310417891753642023.jpg                                                                            |
| File History.lnk                                                                                    | File History                                                                                        |
| E.lnk                                                                                               | E\                                                                                                  |
| D.lnk                                                                                               | D\                                                                                                  |
| BMW-M2-STRIPES.lnk                                                                                  | BMW-M2-STRIPES.jpg                                                                                  |
| Bennett-Mem.dmp.lnk                                                                                 | Bennett-Mem.dmp                                                                                     |
| All Tasks.lnk                                                                                       | Control Panel (All Tasks)                                                                           |

| Property                  | Value                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------|
| Link Target Information   |                                                                                                        |
| Link Target               | 2017-porsche-boxster-facelift-revealed-in-latest-spyshots-has-cayenne-like-tailight-graphics_18.lnk    |
| Type                      | Archive                                                                                                |
| Link Flags                | HasLinkTargetIDList, HasLinkInfo, HasWorkingDir, IsUnicode, DisableLinkTargetIDList                    |
| Target File Size          | 0                                                                                                      |
| Target Path               | D:\2017-porsche-boxster-facelift-revealed-in-latest-spyshots-has-cayenne-like-tailight-graphics_18.lnk |
| Link Attributes           |                                                                                                        |
| Source File Name          | 2017-porsche-boxster-facelift-revealed-in-latest-spyshots-has-cayenne-like-tailight-graphics_18.lnk    |
| LNK Data Size             | 695                                                                                                    |
| Icon Index                | 0                                                                                                      |
| Show Command              | SW_SHOWNORMAL                                                                                          |
| Target System Information |                                                                                                        |
| Drive Type                | DRIVE_REMOVABLE                                                                                        |
| Drive Serial              | C1A1-10FE                                                                                              |
| Volume Label              | SECRET                                                                                                 |
| Local Base Path           | D:\2017-porsche-boxster-facelift-revealed-in-latest-spyshots-has-cayenne-like-tailight-graphics_18.lnk |

### Recent Items

To see recent items, on the toolbar click **Actionable Intel**. In the menu on the left, click **Recent Items** under File Knowledge. The Recent Items view shows information from both macOS and Windows systems.

| User | Type      | Label | Item Name         |
|------|-----------|-------|-------------------|
| josh | Folder    |       | ADSF_FILES        |
| josh | Documents |       | M.PNG             |
| josh | Documents |       | Capture.PNG       |
| josh | Folder    |       | D:\NIGER (D:)     |
| josh | Documents |       | daytona.jpg       |
| josh | Documents |       | bmw_36003.jpg     |
| josh | Documents |       | Pic1.PNG          |
| josh | Documents |       | FatManOnCamel.mkv |
| josh | Folder    |       | Documents         |
| josh | Folder    |       | Special           |
| josh | Documents |       | auktion.csv       |
| josh | Folder    |       | D:\               |
| josh | Documents |       | C-Headlight.jpg   |
| josh | Documents |       | sport.PNG         |

For Windows systems, Recent Items are parsed from information stored in the *NTUSER.DAT* registry files, for example, *\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\*.

For macOS systems, data is parsed from many locations.

| Description                                                                                  | Locations                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Folders                                                                                      | ~/Library/Preferences/com.apple.finder.plist<br>/Library/Preferences/.GlobalPreferences.plist                                                                                                                 |
| Shared File Lists<br>(Documents, Files,<br>Applications,<br>Hosts/Servers,<br>Volumes, etc.) | ~/Library/Applications<br>Support/com.apple.sharedfilelist/com.apple.LSSharedFileList.<MRU Type>.sfl<br>~/Library/Applications<br>Support/com.apple.sharedfilelist/com.apple.LSSharedFileList.<MRU Type>.sfl2 |
| Microsoft Office                                                                             | ~/Library/Preferences/com.microsoft.plist<br>~/Library/Containers/com.microsoft.<Office App<br>Name>/Data/Library/Preferences/com.microsoft.<Office App<br>Name>.securebookmarks.plist                        |
| Volumes                                                                                      | ~/Library/Preferences/com.apple.finder.plist<br>~/Library/Preferences/com.apple.sidebars.plist<br>/private/var/root/Library/Preferences/com.apple.sidebars.plist                                              |
| Files                                                                                        | /.Spotlight-V100/Store-V2/<UUID>/.store.db<br>/private/var/db/Spotlight-V100/BootVolume/Store-V2/<UUID>/.store.db                                                                                             |

The Type column and the Status Bar both show where the information is parsed from.

The screenshot displays the Actionable Intel View interface. On the left, a sidebar lists various data sources such as Device Backups, Account Usage, Cellular Usage, Top Contacts, User Accounts, Downloads, Air Drop, Files, Link Files, File Knowledge, Recent Items, Trash Items, Passwords, Apple Keychain, Program Execution, BAM DMM, Jump Lists, Last Executed, MUI Cache, Notifications, and Prefetch. The main pane shows a table of recent documents, with columns for User, Type, Label, and Item Name. The 'Type' column is highlighted with a red box, showing values like 'Shared File List 2' and 'Recent Documents'. The 'Item Name' column shows various file names, including 'Porsche-Parts.docx', 'Balsalm.png', 'AlliedParts.rtf', 'gone.jpeg', 'Porsche-Parts.doc', 'BMW\_Info.JPG', 'data\_export\_2019-10-09.csv', 'records.xls', and 'auction.csv'. At the bottom, a detailed view of a selected record is shown, displaying its hex, strings, preview, metadata, location, and record data. The 'Record' tab is active, showing the file's path: `/Racer - Data/Users/josh/Library/Application Support/com.apple.sharedfilelist/com.apple.LSSharedFileList.RecentDocuments.sfl2`. The status bar at the bottom indicates the file's location and type.



The Recent Items view shows these columns in addition to the default Tagged State and Evidence ID.

- User
- Type
- Label
- Item Name
- Path
- Mount Path
- Date
- Index Value

The User column is based on the path the data is parsed from. Recent Items parsed from a directory in */Users/<user name>* show <user name> in the User column. Recent Items parsed from files in */private/var/root* show root in the User column. The User column is blank for data parsed from the Spotlight index. The file path is used to populate the User column.

Some columns are not used for all Recent Items parsed. For example, data parsed from shared file lists use the Label and Index Value columns to provide information about:

- Which *LSSharedFileList* the data was parsed from (Label is a portion of the file name of the .slf or .slf2 file)
- Which item number under *\$archiver* the entry was parsed from (Index Value is the Item number for the entry under *Root/\$archiver/items/*).

**Note:** All of the parsed information for an entry can be found in *Root/\$archiver/items/Item <#>/Bookmark* in the Preview sub-view for that file in the File Content view. There may be additional data for the entry in *Root/\$archiver/items/Item <#>/Bookmark*. The Label column is only used for shared file lists.

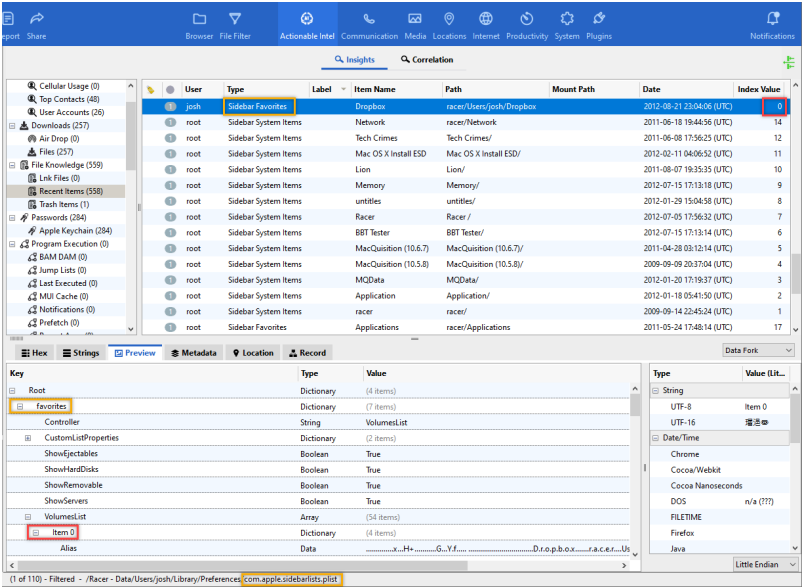
| User | Type             | Label            | Item Name           | Path                                                                                 | Mount Path | Date                      | Index Value |
|------|------------------|------------------|---------------------|--------------------------------------------------------------------------------------|------------|---------------------------|-------------|
| josh | Shared File List | Recent Documents | recentDocs          | file:///Users/josh/Library/MobileDocuments/com-apple-CloudDocs/recentDocs            |            | 2015-07-21 17:56:39 (UTC) | 9           |
| josh | Shared File List | Recent Documents | BMMhwad.slif        | file:///Users/josh/Desktop/BMMhwad.slif                                              |            | 2015-09-14 23:17:53 (UTC) | 8           |
| josh | Shared File List | Recent Documents | RecentPats copy.pdf | file:///Users/josh/Library/MobileDocuments/com-apple-CloudDocs/RecentPats%20copy.pdf |            | 2015-07-21 18:38:49 (UTC) | 7           |
| josh | Shared File List | Recent Documents | recentPats          | file:///Users/josh/Desktop/recentPats                                                |            | 2015-09-14 23:17:53 (UTC) | 6           |
| josh | Shared File List | Recent Documents | IMG_11.png          | file:///Users/josh/Documents/FamilyPhoto/IMG_11.png                                  |            | 2015-11-24 17:58:19 (UTC) | 5           |
| josh | Shared File List | Recent Documents | model-3-recent.jpg  | file:///Users/josh/Desktop/model-3-recent.jpg                                        |            | 2017-09-08 16:52:39 (UTC) | 4           |
| josh | Shared File List | Recent Documents | bookly.slif         | file:///Users/josh/Library/MobileDocuments/com-apple-CloudDocs/bookly.slif           |            | 2015-09-12 12:28:07 (UTC) | 3           |
| josh | Shared File List | Recent Documents | BMMhwad.slif        | file:///Users/josh/Library/MobileDocuments/com-apple-CloudDocs/BMMhwad.slif          |            | 2015-09-14 23:17:53 (UTC) | 2           |
| josh | Shared File List | Recent Documents | ml.jpg              | file:///Users/josh/Desktop/ml.jpg                                                    |            | 2017-09-04 15:54:28 (UTC) | 1           |
| josh | Shared File List | Recent Documents | graham-shop.jpg     | file:///Users/josh/Desktop/graham-shop.jpg                                           |            | 2016-12-15 17:49:05 (UTC) | 0           |
| josh | Shared File List | Recent Documents | gms.jpg             | file:///Users/josh/Desktop/gms.jpg                                                   |            | 2016-02-02 16:20:51 (UTC) | 9           |
| josh | Shared File List | Recent Documents | AlkalPats.slif      | file:///Users/josh/Desktop/AlkalPats.slif                                            |            | 2016-07-03 15:17:39 (UTC) | 8           |
| josh | Shared File List | Recent Documents | Bakal.jpg           | file:///Users/josh/Desktop/Bakal.jpg                                                 |            | 2017-11-30 13:48:18 (UTC) | 7           |
| josh | Shared File List | Recent Documents | Porsche Parts.doc   | file:///Users/josh/Documents/Porsche Parts.doc                                       |            | 2020-09-12 21:07:58 (UTC) | 6           |
| josh | Shared File List | Recent Documents | Porsche Parts.doc   | file:///Users/josh/Library/MobileDocuments/com-apple-CloudDocs/Porsche Parts.doc     |            | 2020-09-22 22:43:08 (UTC) | 5           |
| josh | Shared File List | Recent Documents | RecentPats          | file:///Users/josh/Desktop/RecentPats                                                |            | 2016-06-27 16:16:15 (UTC) | 4           |
| josh | Shared File List | Recent Documents | gms.jpg             | file:///Users/josh/Desktop/gms.jpg                                                   |            | 2016-09-12 14:42:02 (UTC) | 3           |
| josh | Shared File List | Recent Documents | gms.jpg             | file:///Users/josh/Library/MobileDocuments/com-apple-CloudDocs/gms.jpg               |            | 2020-01-02 18:54:02 (UTC) | 2           |
| josh | Shared File List | Recent Documents | Finance.slif        | file:///Users/josh/Library/MobileDocuments/com-apple-CloudDocs/Finance.slif          |            | 2015-07-02 19:23:02 (UTC) | 1           |
| josh | Shared File List | Recent Documents | bookly.slif         | file:///Users/josh/Library/MobileDocuments/com-apple-CloudDocs/bookly.slif           |            | 2015-09-12 12:28:07 (UTC) | 0           |

| Key                | Value                         |
|--------------------|-------------------------------|
| Root               | Dictionary (10 items)         |
| Searcher           | NSMachOClass (10 items)       |
| Items              | NSMachOClass (10 items)       |
| Item 0             | NSMachOClass (10 items)       |
| Item 1             | NSMachOClass (10 items)       |
| Item 2             | NSMachOClass (10 items)       |
| Item 3             | NSMachOClass (10 items)       |
| Item 4             | NSMachOClass (10 items)       |
| Bookmark           | Bookmark (10 items)           |
| Creation Options   | Creation Options (10 items)   |
| Display Name       | Display Name (10 items)       |
| File Creation Date | File Creation Date (10 items) |

**Tip:** Parsed information can be tagged from the Content pane. Additional data can also be tagged from the File Content view.

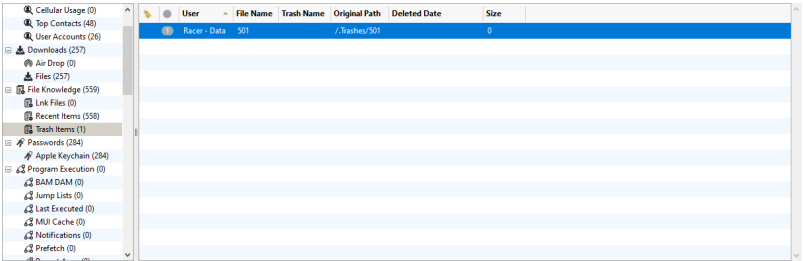
The same principle is used for other data parsed from plist files, but instead of the Label column, the Type column is used. The Type column, generated by Inspector, can be a combination of the plist filename and plist entry. For example, data is parsed from both `/Root/favorites` and `/Root/systemitems` in `com.apple.sidebarlists.plist`. Entries parsed will be labeled as Sidebar Favorites or Sidebar System Items, depending on the plist entry it is parsed from.



The Type for data parsed from Microsoft securebookmarks plists is based on the name of the plist.

## Trash Items

Choosing Trash Items in the File Knowledge sub-view menu reveals items in stored in the `.Trash` folders for macOS and Recycle Bin folders for Windows. Since the Windows Recycle Bin maintains more information about files, some columns listed in this view pertain to Windows Recycle Bin records only (Trash Name and Deleted Date).

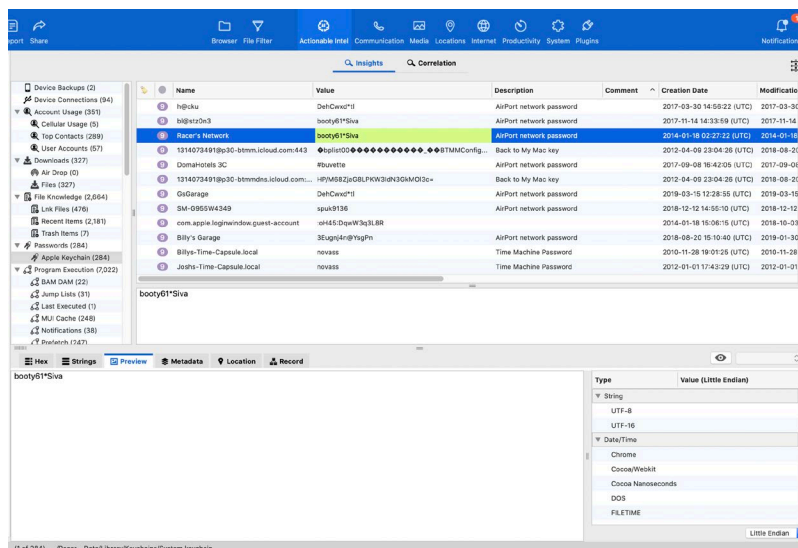


# Passwords

In Actionable Intel, Passwords offers a view of parsed Apple Keychain data from macOS and iOS. Keychains are processed during initial evidence ingestion. Inspector identifies these by file extension (.keychain or .keychain-db). In macOS, there is a system keychain as well as user keychains. The system keychains typically store Wi-Fi passwords and Time Machine passwords. Users' login keychains can contain a variety of data and are typically unlocked with the user's login passwords.

While passwords are needed to unlock some keychain data, without any passwords Inspector parses all of the information stored in the System keychain and all data except the Value stored in locked user login keychains.

This image shows system keychain data with no password.



**Note:** For Apple Keychain entries, you can select an entry in one column (see the highlighted green data). Only the highlighted data appears in the lower portion of the Content pane. With a Keychain entry selected in the Content pane, click **Preview** in the File Content view. The contents of the Value column are shown. If the Value column contains a binary property list, the property list is parsed in the Preview tab in the File Content view. The contents of the Value column can be copied from the lower portion of the Content pane (if that field is highlighted), or from the Preview tab.

This image shows user login keychain data with no password.

| Name                                                         | Value | Description       | Comment                           | Creation Date             | Modification |
|--------------------------------------------------------------|-------|-------------------|-----------------------------------|---------------------------|--------------|
| Apple Persistent State Encryption                            |       |                   | Used by the persistent state f... | 2012-01-02 02:21:47 (UTC) | 2020-05-...  |
| Apple Persistent State Encryption                            |       |                   | Used by the persistent state f... | 2012-01-02 02:21:47 (UTC) | 2020-05-...  |
| www.facebook.com (jbenett_mac@me.com)                        |       | Web form password | default                           | 2014-01-05 00:34:46 (UTC) | 2014-01-0... |
| www.facebook.com (jbenett_mac@me.com)                        |       | Web form password | default                           | 2014-01-05 00:34:46 (UTC) | 2014-01-0... |
| www.facebook.com (jbenett_mac@me.com)                        |       | Web form password | default                           | 2014-01-05 00:34:46 (UTC) | 2014-01-0... |
| MSN (jbenett_mac@hotmail.com)                                |       |                   |                                   | 2010-02-15 23:15:15 (UTC) | 2010-02-1... |
| Adium                                                        |       |                   |                                   | 2010-11-29 01:53:31 (UTC) | 2010-11-2... |
| Facebook (jbenett_mac@me.com)                                |       |                   |                                   | 2010-11-29 01:53:31 (UTC) | 2010-11-2... |
| OTalk (joshbarnettcar@gmail.com)                             |       |                   |                                   | 2010-11-29 01:46:50 (UTC) | 2010-11-2... |
| com.apple.account.itsm.token                                 |       |                   |                                   | 2016-12-07 19:57:10 (UTC) | 2016-12-0... |
| BackupIDSAccountToken (jbenett_mac@icloud.com-AuthTok...     |       |                   |                                   | 2016-07-05 20:05:01 (UTC) | 2016-07-0... |
| Phone Backup                                                 |       |                   |                                   | 2016-07-26 11:22:23 (UTC) | 2016-10-...  |
| com.apple.gs.itsm.pst.com.apple.account.AppleIDAuthentica... |       |                   |                                   | 2016-12-07 19:57:10 (UTC) | 2016-12-0... |
| com.apple.gs.itsm.hs.com.apple.account.AppleIDAuthentica...  |       |                   |                                   | 2016-12-07 19:57:10 (UTC) | 2016-12-0... |
| its.message-protection-public-data-registered                |       |                   |                                   | 2016-04-05 20:18:17 (UTC) | 2016-10-...  |
| com.apple.facetime.registrationV1                            |       |                   |                                   | 2014-03-18 23:12:32 (UTC) | 2016-10-...  |

If no passwords are entered at initial evidence ingestion, Inspector will process and display only the data accessible without a password. If passwords are discovered later, you can either reprocess the entire case or export the keychain files from the case and reprocess only the keychain files.

**Tip:** One approach to unlock keychain data is to initially ingest the evidence with only Actionable Intel selected for the Extract Data processing option. No other processing options should be selected. Data is quickly ingested, and any passwords parsed from the System keychain are viewable.

Create a password list based on the data parsed from the System keychain. Create a new case file, add the passwords in Manage Passwords, and process the case with only Actionable Intel selected for the Extract Data processing option. Compare previous Apple Keychain data in the Passwords sub-view to determine if any login keychains were unlocked.

This can be an iterative process, performed with new passwords lists. To decrease processing time, if there are plans to iteratively attack keychain passwords, export the keychains files and re-process only the keychains as new passwords are added. The easiest way to do this is to use a File Filter to locate all keychain files, and then export them.

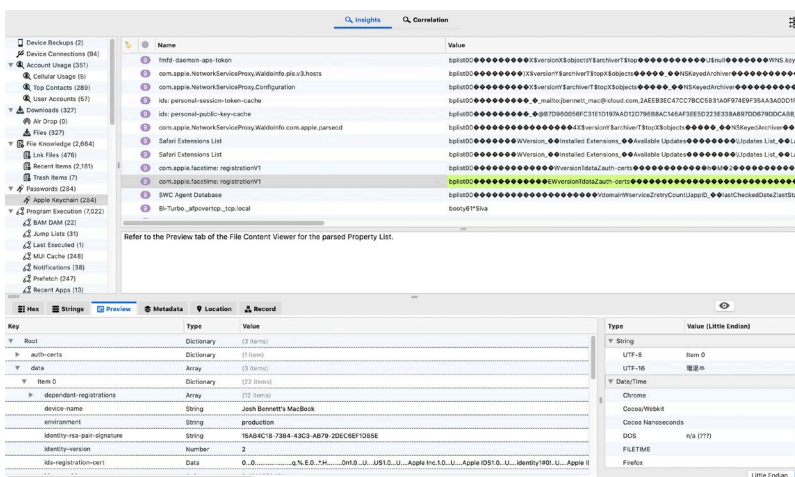
Some rules to know before adding passwords:

- Passwords are tried in the order they are entered. In the Passwords window, they are shown in alphabetical order.
- Passwords must be UTF-8 encoded. An error message will be displayed for non-UTF-8 encoded passwords.
- A password list can be imported. The list must be UTF-8 encoded with one password per line.
- Long password lists can take significant time to run. For example, 14 million passwords take roughly 4 hours per keychain file.
- When manually entering passwords, leading and trailing spaces will be truncated.

As Inspector processes keychain files, once a password successfully unlocks the data, no further passwords are attempted for that keychain.

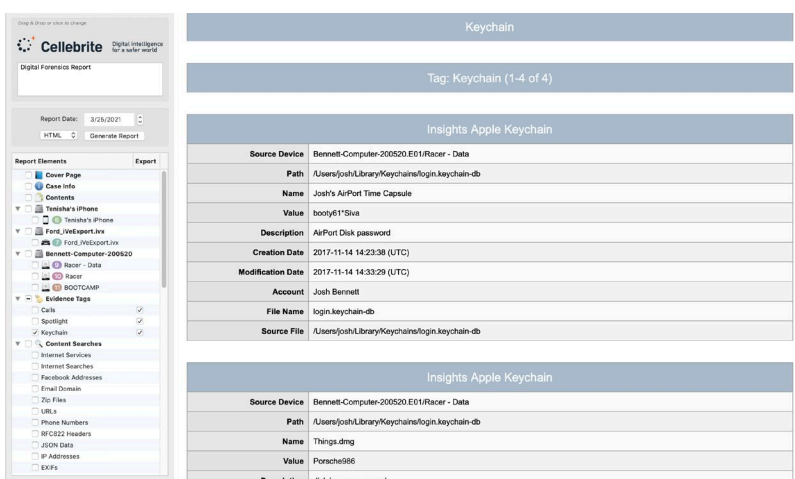
## Viewing Keychain Data

With a Keychain entry selected in the Content pane, click **Preview** in the File Content view. The contents of the Value column are displayed. For keychains storing property list data in the Value field, when the Value field is highlighted in the Content pane and the Preview tab, the property list is parsed in the Preview tab.



## Tagging and Reporting Keychain Data

Data from Apple Keychains can be tagged for inclusion in the examination report. In the report, only columns containing data will be shown, so if a Keychain is locked and the Value cannot be parsed for the entry, it will not be shown in the report. Similarly, if there is no data in the Description column it will not be shown in the report.



## Program Execution

In Actionable Intel, Program Execution offers a view of evidence of applications that have been launched by a user. This sub-view is specific to Windows. The artifacts in this table are parsed in the Program Execution sub-view menu.

| Artifact                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Background Activity Moderator (BAM) and Desktop Activity Moderator (DAM) | Information stored in the Windows registry (Windows 10) that tracks executables run by each user on the system. BAM controls activity of background applications. DAM was created to ensure consistent long battery life. DAM information is stored only on tablets and mobile devices. Each BAM/DAM entry provides insights into the applications run by the user identified in the SID column entry.                                                                                                                                                 |
| Jump Lists                                                               | Jumplists are created by the operating system (Windows 7 and above) based on user actions. They give the user quick access to recently accessed application files and actions.                                                                                                                                                                                                                                                                                                                                                                         |
| Last Executed                                                            | This shows the specific executable used by an application to open the files documented in the OpenSaveMRU key. In addition, each value also tracks the directory location for the last file that was accessed by that application.                                                                                                                                                                                                                                                                                                                     |
| Multilingual User Interface (MUI) Cache                                  | Each time a new application is started on Windows system, the application name and a description are stored in a registry key.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Notifications                                                            | A history of notifications sent to users.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Prefetch                                                                 | Prefetching was introduced with Windows XP to minimize seek times on hard disks by loading into memory certain data that is needed for booting and launching applications. In this sub-view, Inspector lists the application filenames in the top of the Content pane (along with run counts and times) and associated DLL (Dynamic Link Library) files in the bottom of the Content pane. Filters can be applied to the data contained in the top of the Content pane by selecting the Show Filter button and applying the desired filter parameters. |
| Recent Apps                                                              | Data stored in NTUSER.dat, recording information about applications recently used and the files accessed by the apps.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ShimCache                                                                | A mechanism in Windows to support older apps on new version of Windows. Provides information about executables.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Superfetch                                                               | Introduced with Windows Vista, stores launch times and preloads applications into memory based on a given user's previous usage patterns. Inspector displays the volume name, entry name, and run time for each item.                                                                                                                                                                                                                                                                                                                                  |

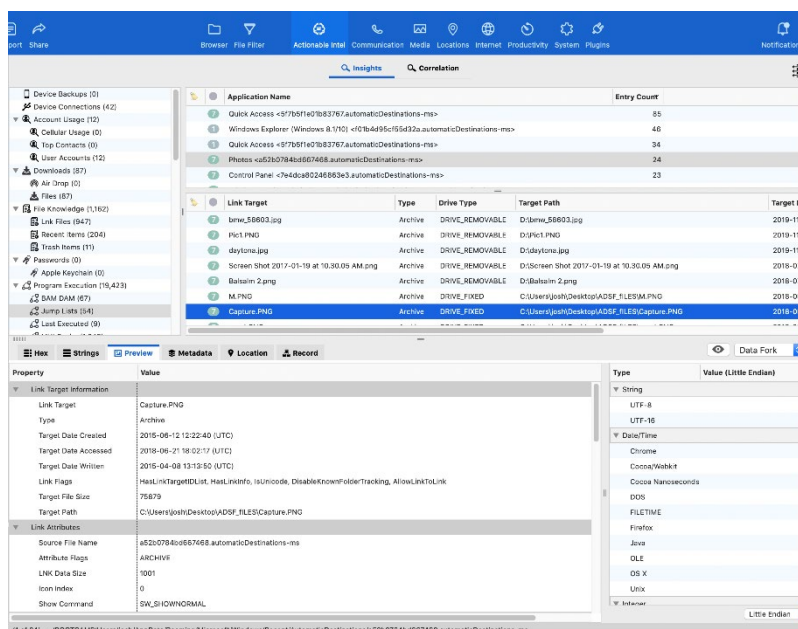
| Artifact                             | Description                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Assist                          | This shows applications the user has launched, and the data is parsed from NTUSER.DAT. Information can be used to determine: frequency of program execution for each user account, last time a program was launched, where the program was launched from, information about programs that have been deleted or uninstalled from the system, and proof of the existence of data in a location that is no longer available. |
| Windows Activity Timeline            | Tracks user Activities, e.g. website accesses, program executions, files accessed by programs, and when particular apps were in focus.                                                                                                                                                                                                                                                                                    |
| AmCache                              | Stores metadata about ShimCache executables that have been run, program installed, and devices connected.                                                                                                                                                                                                                                                                                                                 |
| ComDlg32                             | Tracks when the user used the Open/Save dialog box to open or save a file.                                                                                                                                                                                                                                                                                                                                                |
| System Resource Usage Monitor (SRUM) | Monitors desktop applications, services, windows apps, and network connections. SRUM data is stored in the Windows registry, with historic information contained in a database. Some information tracked includes: network connectivity, network data usage, application resource usage, Windows push notification, and energy use.                                                                                       |

To see any of these artifacts, on the toolbar click **Actionable Intel**. In the menu on the left, click the appropriate artifact category under Program Execution. For some artifacts, additional information is parsed by Inspector; the Content pane splits to show additional data. The most complex is Jump Lists.

Select the jump list that was created for a particular application. For that jump list, the bottom portion of the Content pane shows Link Targets, Type, Drive Type, Target Path, Target Date Accessed, Target Date Created, and Target Date Written.

Select an item in the bottom portion of the Content pane. In the File Content view, click **Preview** to see information relating to the item.

Information can be tagged for reporting purposes from individual rows shown in the File Content view. Additionally, you can use Find in the Content pane.





# Search

In Actionable Intel, Search offers a view of parsed search data from macOS and Windows.

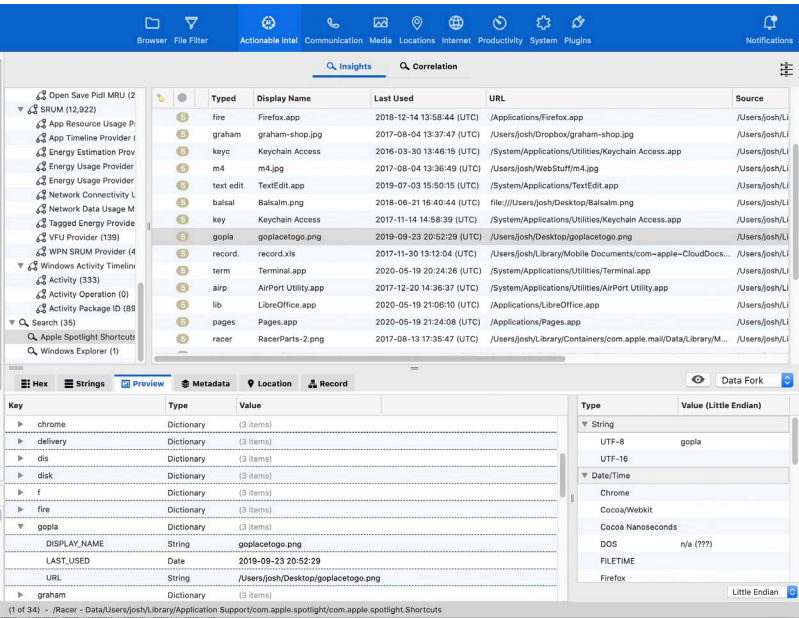
In macOS, Apple Spotlight Shortcuts are parsed and displayed. When a user on a Mac computer presses CMD+SPACEBAR, Spotlight Search appears.



As the user begins typing, Spotlight provides recommendations based on the characters typed. The user can choose a suggestion before they have finished typing the entire word or string. That information is stored in `~/Library/Application Support/com.apple.spotlight/com.apple.spotlight.Shortcuts`. Parsed data shows this information.

- the user account the data was parsed from (User)
- what the user typed (Typed)
- what Spotlight displayed for the item the user selected (Display Name)
- the Last Used timestamp
- the location of the selected item such as the path for apps, path for files, URLs for websites, and more (URL)
- the file the data was parsed from (Source)

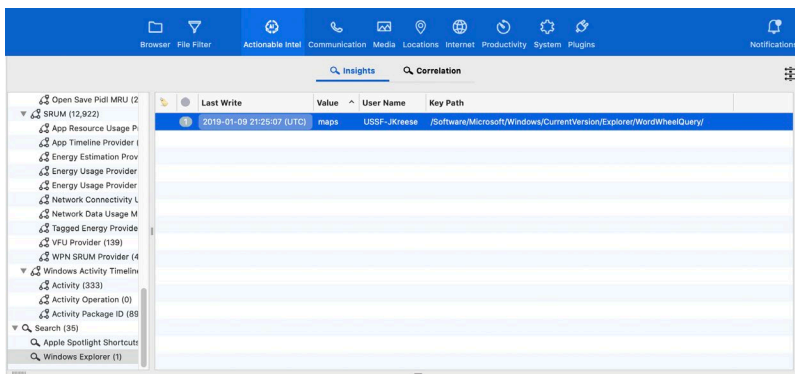
To see searched items from a Mac computer, in the toolbar click **Actionable Intel**, then in the menu on the left, click **Apple Spotlight Shortcuts** under Search.



To see searched items from a Windows computer, in the toolbar click **Actionable Intel**, then in the menu on the left, click **Windows Explorer** under Search.



For Windows, Windows Explorer search artifacts are parsed and displayed. In Windows 7 and Windows 10, this data is stored in *NTUSER.dat* in the *WordWheelQuery* key.



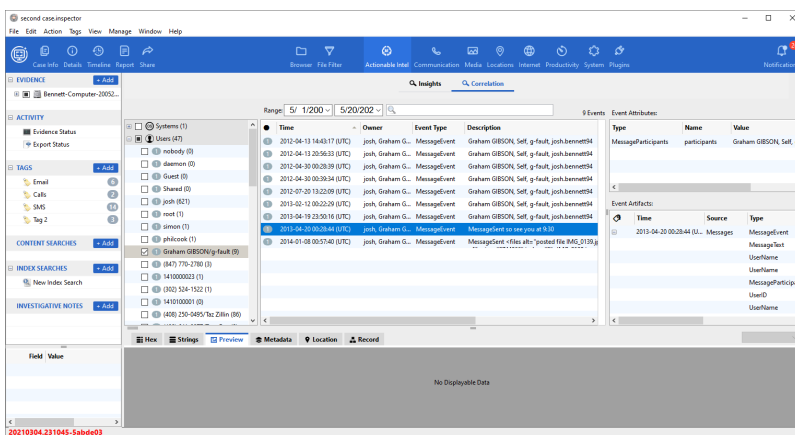
## Activity Correlation

The Correlation view in Actionable Intel makes it easy to see the story of an entity's activity.

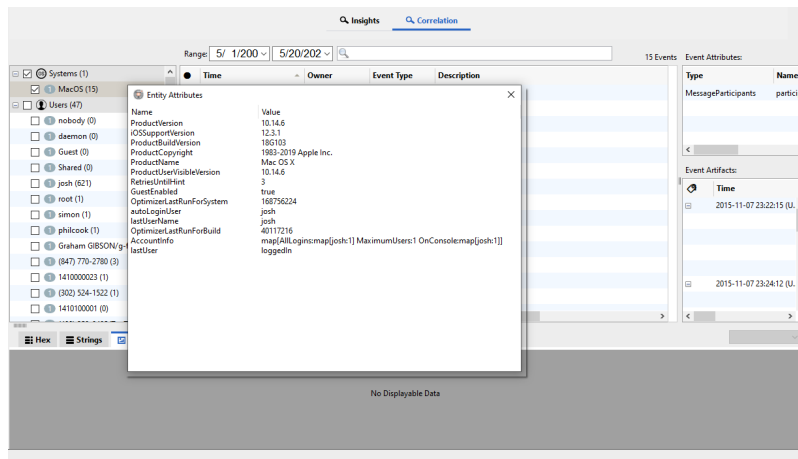
**Note:** The correlation engine only works on images from Windows-based systems.

You can easily see, filter, and pivot on all correlated events, whether they were done by a user or by the system. There are three types of entities: System, User, and Device. These entities are listed in the left column of the Correlation view and can be enabled or disabled as necessary. The number of correlated events is shown in parenthesis after each entity's name.

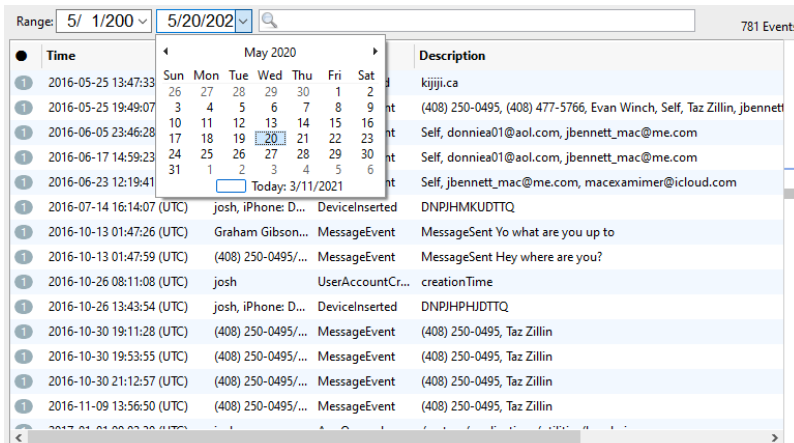
You can run the Correlation engine during initial ingestion or afterward by selecting **Correlation** from the **Evidence Status** view.



Each entity can have one or many events associated with it. Each entity also has its own attributes, which you can see by double-clicking the entity or pressing SPACEBAR. This lets you quickly see attributes like when an operating system was installed, the specific version, the registered owner, and more.



The middle pane of the Correlation view shows a list of all the events, and includes the time of each event, the owner of each event, the type of event, and a full description. This list can be shortened by deselecting any of the entities in the list. It is also possible to filter these events based on time and date. This will only show events between the selected dates.



You can search on keywords, which are then highlighted in the event list. The scrollbar marks where the keywords exist in the list so you can quickly scroll to the marks to see each instance of the highlighted keyword.

Range: 5/ 1/200 | 5/20/202 | gibby 781 Events

Systems (1)

MacOS (5)

Users (47)

Devices (39)

|  | Time                      | Owner               | Event Type       | Description                                                             |
|--|---------------------------|---------------------|------------------|-------------------------------------------------------------------------|
|  | 2016-05-25 13:47:33 (UTC) | josh                | URLAccessed      | kijji.ca                                                                |
|  | 2016-05-25 19:49:07 (UTC) | josh, (408) 250-... | MessageEvent     | (408) 250-0495, (408) 477-5766, Evan Winch, Self, Taz Zillan, jbenne... |
|  | 2016-06-05 23:46:28 (UTC) | josh, donniea01...  | MessageEvent     | Self, donniea01@aol.com, jbenne...mac@me.com                            |
|  | 2016-06-17 14:59:23 (UTC) | josh, donniea01...  | MessageEvent     | Self, donniea01@aol.com, jbenne...mac@me.com                            |
|  | 2016-06-23 12:19:41 (UTC) | josh, macexamim...  | MessageEvent     | Self, jbenne...mac@me.com, macexamimer@icloud.com                       |
|  | 2016-07-14 16:14:07 (UTC) | josh, iPhone: D...  | DeviceInserted   | DNPIHMKUDDTQ                                                            |
|  | 2016-10-13 01:47:26 (UTC) | Graham Gibson...    | MessageEvent     | MessageSent Yo what are you up to                                       |
|  | 2016-10-13 01:47:59 (UTC) | (408) 250-0495/...  | MessageEvent     | MessageSent Hey where are you?                                          |
|  | 2016-10-26 08:11:08 (UTC) | josh                | UserAccountCr... | creationTime                                                            |
|  | 2016-10-26 13:43:54 (UTC) | josh, iPhone: D...  | DeviceInserted   | DNPIHPHJDTTQ                                                            |
|  | 2016-10-30 19:11:28 (UTC) | (408) 250-0495/...  | MessageEvent     | (408) 250-0495, Taz Zillan                                              |
|  | 2016-10-30 19:53:55 (UTC) | (408) 250-0495/...  | MessageEvent     | (408) 250-0495, Taz Zillan                                              |
|  | 2016-10-30 21:12:57 (UTC) | (408) 250-0495/...  | MessageEvent     | (408) 250-0495, Taz Zillan                                              |
|  | 2016-11-09 13:56:50 (UTC) | (408) 250-0495/...  | MessageEvent     | (408) 250-0495, Taz Zillan                                              |

In the right side of the Correlation view, you can see Event Attributes and Event Artifacts. Event Attributes provides information about the selected event such as its type, its name, and its value, for example file path, file name, and so forth. Event Artifacts shows all the artifacts that are associated with the selected event. For example, if the file *bobbyR.txt* was accessed by the user Gibby, you can see the path for that file, the user who accessed it, the drive it was on, and in this case the Windows jumplist entry that was created for it.

| Event Attributes: |            |               |
|-------------------|------------|---------------|
| Type              | Name       | Value         |
| FilePath          | TargetPath | F:\bobbyR.txt |

| Event Artifacts:     |              |                      |                     |  |
|----------------------|--------------|----------------------|---------------------|--|
| Source               | Type         | Name                 | Description / Value |  |
| 1:31:23 (... JMPLIST | FileAccessed |                      | F:\bobbyR.txt       |  |
|                      | FilePath     | TargetPath           | F:\bobbyR.txt       |  |
|                      | UserName     | UserName             | Gibby               |  |
|                      | FileName     | TargetName           | bobbyR.txt          |  |
|                      | FileName     | NormalizedFileName   | bobbyR.txt          |  |
|                      | FileFolder   | NormalizedFileFolder | F:                  |  |

To pivot to the created jumplist so you can view other items, open the context menu on any of the items in Event Artifacts and click **Reveal > Item in Native View**.

## Plugins View

The Plugins view provides access to other tools integrated into Inspector. At this time, the Plugin Manager provides a way to integrate Apple Pattern of Life Lazy Output'er (APOLLO) into Inspector.

To view plugins installed in Inspector, or to update to a newer version of a plugin, click **Manage > Plugins**. The Manage Plugins window shows all installed plugins and the source and version number for each.



In the Manage Plugins window, you can install and remove plugins from Inspector. To install a newer version of a plugin, you must first select the plugin and click **Remove**.

This chapter provides this topic about the Plugins View.

- [APOLLO Plugin](#)

## APOLLO Plugin

APOLLO, written by Sarah Edwards, is a python script which runs a series of queries against the SQLite databases on iOS devices. APOLLO's power is in the SQL queries, each query designed to look at specific iOS data. The queries are categories by function and stored in text files. APOLLO aims to easily correlate multiple databases with hundreds of thousands of records in order to determine what has happened on the device. For more information, see the series of blog posts by Sarah Edwards at <https://www.mac4n6.com/blog/>.

APOLLO is included in the Inspector installer and will install into these directories.

- macOS:  
*/Users/<username>/Library/Application Support/Cellebrite/Inspector/Plugins/APOLLO-master*
- Windows 10:  
*C:\Users\<username>\AppData\Roaming\Cellebrite\Inspector\Plugins\APOLLO-master*

## Get a new version of the APOLLO Plugin

1. Download a zip archive of the APOLLO modules file from <https://github.com/mac4n6/APOLLO>.
2. In the Mange Plugins window, select the APOLLO plugin and click **Remove**.
3. Click **Install** and select the APOLLO zip archive.

## Use the APOLLO Plugin

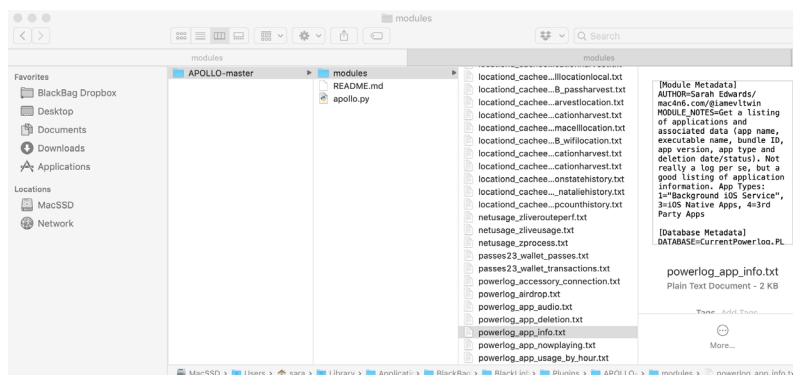
1. Import a macOS or iOS device into Inspector.
2. Select the device in the Component list.
3. On the toolbar, click **Plugins**.

The APOLLO queries run, and results are shown in the Content pane.

The queries in APOLLO are categorized based on what data is queried. Inspector separates APOLLO data into each category and displays the results of each query.

| Start                     | End                       | Bundle Id        | Group Id   | Activity Type                 | Content Description         | User Activity Required |
|---------------------------|---------------------------|------------------|------------|-------------------------------|-----------------------------|------------------------|
| 2020-04-27 21:38:25 (UTC) | 2020-04-27 21:38:25 (UTC) | com.apple.mail   |            | com.apple.mail.mailbox        | v1.0/com.apple.mail.mailbox |                        |
| 2020-04-27 21:38:25 (UTC) | 2020-04-27 21:38:25 (UTC) | com.apple.mail   |            | com.apple.mail.mailbox        | v1.0/com.apple.mail.mailbox |                        |
| 2020-04-27 21:38:25 (UTC) | 2020-04-27 21:38:25 (UTC) | com.apple.mail   |            | com.apple.mail.message        | v1.0/com.apple.mail.message |                        |
| 2020-04-27 21:38:25 (UTC) | 2020-04-27 21:38:25 (UTC) | com.apple.mail   |            | com.apple.mail.message        | v1.0/com.apple.mail.message |                        |
| 2020-04-27 21:38:25 (UTC) | 2020-04-27 21:38:25 (UTC) | com.apple.mail   |            | com.apple.mail.message        | v1.0/com.apple.mail.message |                        |
| 2020-04-27 21:38:30 (UTC) | 2020-04-27 21:38:30 (UTC) | com.apple.mail   |            | com.apple.mail.message        | v1.0/com.apple.mail.message |                        |
| 2020-04-27 21:39:00 (UTC) | 2020-04-27 21:39:00 (UTC) | com.apple.Safari | com.app... | google.com/searchclient...    | v1.0/NSUserActivityType...  |                        |
| 2020-04-27 21:39:10 (UTC) | 2020-04-27 21:39:10 (UTC) | com.apple.Safari | com.app... | shift.com/cars/san-francis... | v1.0/NSUserActivityType...  |                        |
| 2020-04-29 17:54:40 (UTC) | 2020-04-29 17:54:40 (UTC) | com.apple.Safari | com.app... | google.com/searchclient...    | v1.0/NSUserActivityType...  |                        |
| 2020-04-29 17:54:55 (UTC) | 2020-04-29 17:54:55 (UTC) | com.apple.Safari | com.app... | pelicanparts.com/Porsche...   | v1.0/NSUserActivityType...  |                        |
| 2020-04-29 17:55:25 (UTC) | 2020-04-29 17:55:25 (UTC) | com.apple.Safari | com.app... | forums.pelicanparts.com/...   | v1.0/NSUserActivityType...  |                        |
| 2020-04-29 17:55:40 (UTC) | 2020-04-29 17:55:40 (UTC) | com.apple.Safari | com.app... | pelicanparts.com/Porsche...   | v1.0/NSUserActivityType...  |                        |
| 2020-04-29 17:55:55 (UTC) | 2020-04-29 17:55:55 (UTC) | com.apple.Safari | com.app... | pelicanparts.com/Porsche...   | v1.0/NSUserActivityType...  |                        |
| 2020-04-29 17:56:35 (UTC) | 2020-04-29 17:56:35 (UTC) | com.apple.Safari | com.app... | pelicanparts.com/catalog...   | v1.0/NSUserActivityType...  |                        |
| 2020-04-29 17:56:55 (UTC) | 2020-04-29 17:56:55 (UTC) | com.apple.Safari | com.app... | pelicanparts.com/catalog...   | v1.0/NSUserActivityType...  |                        |
| 2020-04-29 17:57:05 (UTC) | 2020-04-29 17:57:05 (UTC) | com.apple.Safari | com.app... | pelicanparts.com/catalog...   | v1.0/NSUserActivityType...  |                        |

To see the query used, view the text files associated with the query stored in the APOLLO-master directory.



# Tags

During a forensic analysis, you can tag items of interest. Tagged data can then be included in the examiner report. Individually tagged items are stored within tags. Tags are used to organize a group of similar or related items.

This chapter provides these topics about tagging in Inspector.

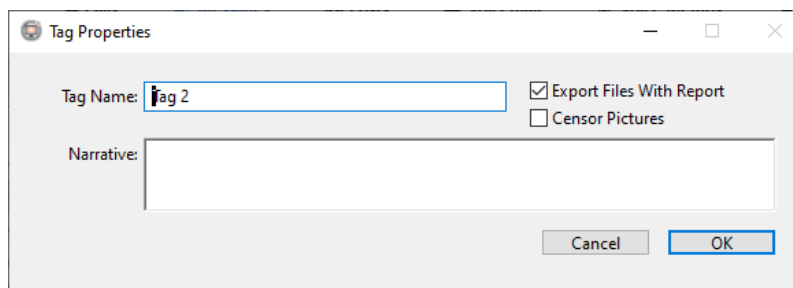
- [Adding Tags](#)
- [Configure Metadata for Tags](#)
- [Tagging Evidence](#)
- [Tags View](#)
- [Deleting Tags](#)

## Adding Tags

There are several ways to create tags.

1. You can create tags in large batches if you have a plan in mind, or you can create tags during the course of an examination as you select items of interest.
  - In the Component list to the right of TAGS, click **Add**.
  - In any Inspector view, select an item of interest, then choose either of these actions.
    - On the menu bar, click **Tags > Tag <artifact> As**, where <artifact> is the type of item you selected, and then click **New Tag**.
    - Open the context menu with that item selected, then click **Tag <artifact> As**, where <artifact> is the type of item you selected, and then click **New Tag**.

A new empty tag is created that you can name and describe.



The default name is Tag <#>, where <#> is an incremental number.

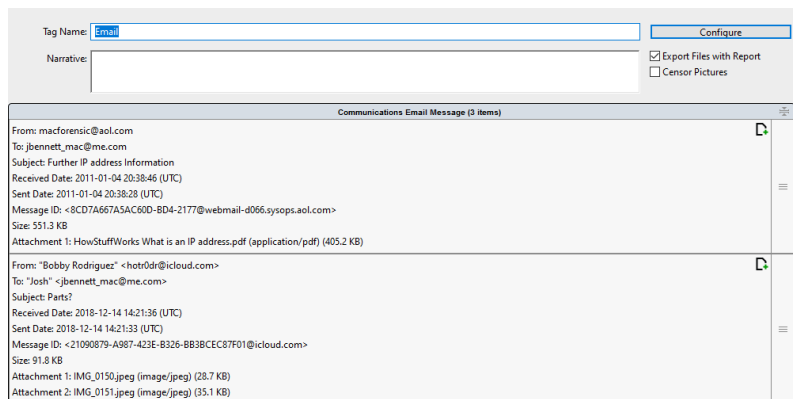
2. Either in the Tags section of the Component list, select a tag and type a name in the **Tag Name** field, or in the Tag Properties dialog box type a name in the **Tag Name** field. The tag's default name is overwritten with the new name. You can rename any tag this way any time you like.
3. In the **Narrative** field, add a narrative to describe either the contents of the tag or the reason you created the tag.

Pictures, text messages, calls, .plist info, and so forth can all be tagged. Keep the examiner report in mind while you tag items. Tag similar items with the same tag to keep them together in the report. For instance, use tags to group pictures (one for censored and one for uncensored pictures), phone data, or Internet files together.

## Configure Metadata for Tags

You can edit tags to choose the metadata to include for all files under each tag. Editing tags is faster and more efficient than proving this same information item-by-item. This allows you to choose metadata before you make a case report rather than when each tag is created.

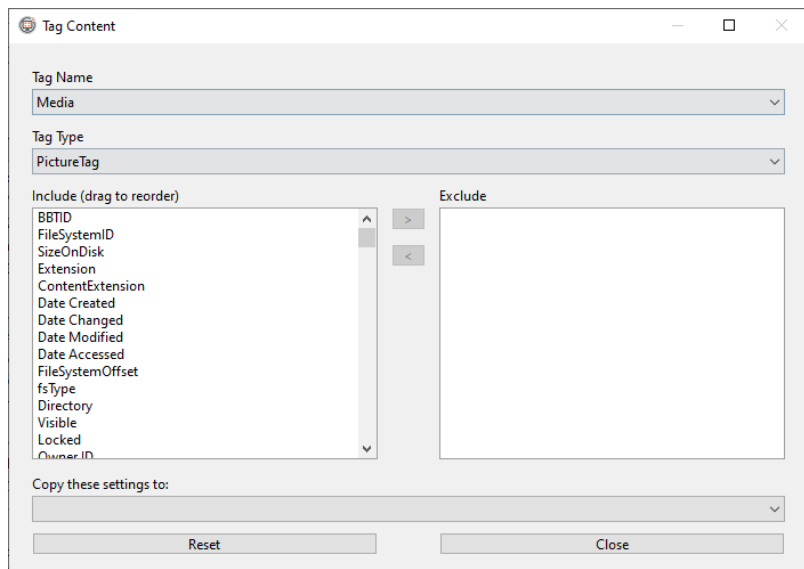
In the Tag view, click **Configure** to choose specific metadata to include.



The Tag Content dialog box appears.

When you configure a tag, any metadata that is available across all tag types appears in the Include list. By default, the current tag name is shown along with the tag type. You can also copy these settings to other tags. To arrange metadata for a tag in order of importance, you can drag and drop them in the Include list.

This order determines how they appear in the Tag view and thus the report.



The Tag view shows specific metadata items that are included by default along with the number of metadata items that can be included.

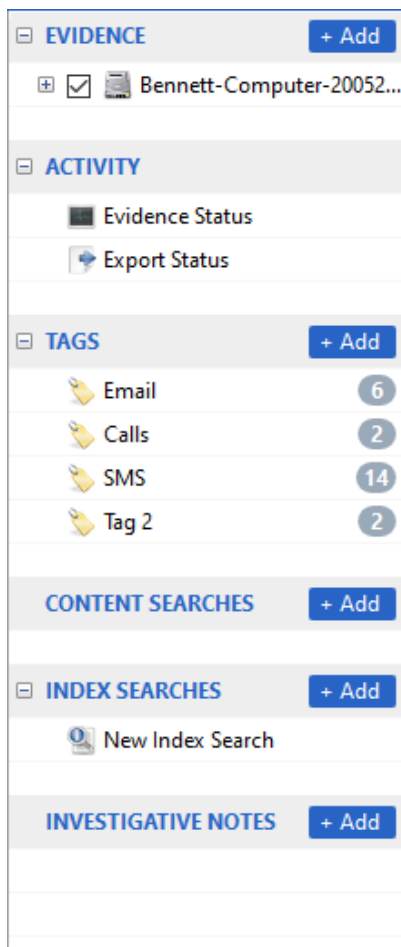
## Tagging Evidence

Inspector automatically assigns a keyboard shortcut to each new tag as it is created. For example, the first tag's shortcut is CMD+1 (Mac) or CTRL+1 (Windows), the second tag's shortcut is CMD+2 or CTRL+2, and so forth.

There are many ways to tag evidence. Begin by selecting any item from one of the panes or views in the Case window, then use whichever approach you prefer.

- On the menu bar, click **Tags > Tag <Item Type> As**.
- Open the context menu and click **Tag <Item Type> As**.
- Drag and drop the item from the Case window onto an existing tag.
- Press the shortcut keys for a specific tag. To see shortcut keys for all the tags in the Component list, select an evidence item and then hold down the CMD key (Mac) or the CTRL key (Windows).
- Press the shortcut keys for the tag last used, CMD+T (Mac) or CTRL+T (Windows).

**Note:** The label of the Tag <Item Type> As menu option reflects the type of item you have selected. For example, if a .plist item is selected for tagging, the label of the menu option is Tag Plist Data As. If an SQLite database element is selected for tagging, the label changes to Tag SQLite Record As.



Tagged files are marked with a tag icon.

In the Tags section of the Component list, a number badge shows how many items each tag contains.



## Tagging File Content

You can tag a piece of file content or parsed information without tagging the entire file. This is useful to tag items of interest parsed by Inspector or contained within .plist files, SQLite databases, and so forth.

For each category in Actionable Intel, there is a corresponding tagging submenu (such as Device Backups, Device Connections, Air Drop, Apple Keychain, Apple Spotlight Shortcuts, and so on). Similarly, there are corresponding tagging submenus for each sub-view in Communications, Locations, Internet, Productivity, and System. Data tagged from Plugins is tagged as the data type Plugins.

These are the other content-aware data types.

| Content       | Description                                    |
|---------------|------------------------------------------------|
| Plist Data    | Individual items from within a Plist file      |
| SQLite Record | Individual record from with an SQLite database |
| Hex Data      | Hexadecimal data                               |
| Text          | Highlighted text                               |

Under most circumstances, the parent file containing tagged file content is marked with a tag icon to indicate it contains tagged content. A single tagged .plist file item or a single tagged database record also has a tag icon that is visible in the File Content view, but some tagged content items, including tagged text snippets and hex data, do not.

Tagged .plist items may appear to have some numbering inconsistencies. For example, if a single .plist item is tagged as item number 4, it may appear in Tags view and Case Report view as item number 0. This happens because .plist files store data in arrays. Data in these arrays are not stored with corresponding numerical values.

## Tagging Email

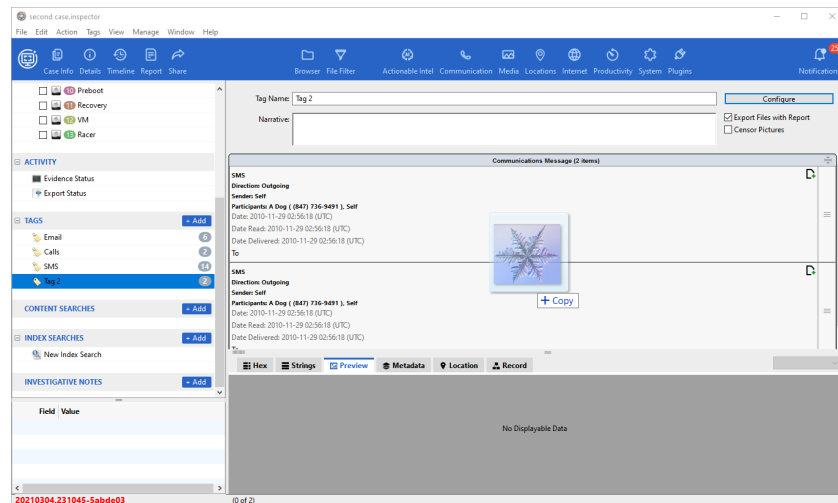
If email previews must be included in the examiner report, you must tag the email from within the Email sub-view of the Communications view or from Index Search when the **Type** field is **Email**. Email tagged in any other view, such as File Filter or in search results, does not result in previews in a report. For more information, see these topics.

- [Inspector Preferences or Options](#)
- [Generating and Exporting the Examiner Report](#)

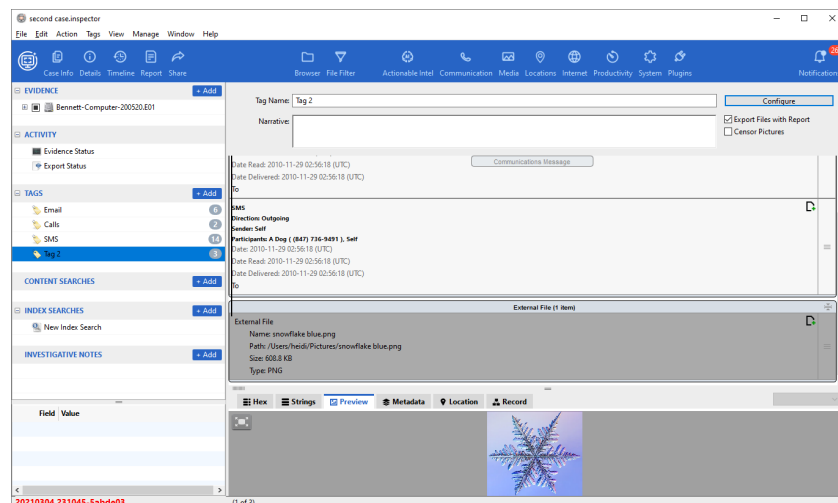
## Tagging External Content

External items such as a screenshot can be tagged and added to the case if necessary.

If a file cannot be displayed in Inspector, export the file and open it in its native application. Take a screenshot and save it to the desktop. Select the appropriate tag in the Component list. Drag the file from the desktop and drop it into the Content pane.



The file is added to the selected tag as external content.



The only way to add external content to an Inspector case is by using this drag-and-drop method.

**Note:** Any internal file on an Inspector case device may also be tagged using this drag-and-drop method. The Tag view is displayed when a tag is selected in the Component list.

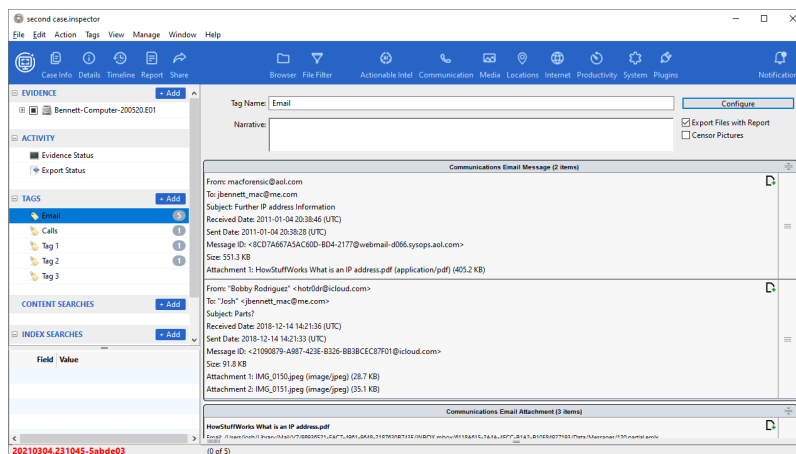
**Note:** Windows users must make a Registry change to enable the drag-and-drop functionality. Inspector requires escalated privileges to run, and because of that, User Account Control in Windows will not allow a lower-privileged program such as Windows Explorer to interact with Inspector. To enable tagging of external content on a Windows system, change this User Account Control setting. In the Registry Editor, navigate to HKEY\_LOCAL\_MACHINE > SOFTWARE >

Microsoft > Windows > CurrentVersion > Policies > System. Double-click the **EnableLUA** key and change the value from 1 to 0.

The process of tagging large amounts of items happens in the background, which allows you to accomplish other work in the case. If you close the case while tagging is still happening in the background, you can choose to keep the case open so you don't lose all items still in process.

## Tags View

The Tags view is one of the most important views in Inspector. This is where evidence is organized before the examiner's report is created. For more information, see [Reporting](#).



The Tags view is blank until tagged evidence is added. As tagged evidence is added, the Content pane is populated.

These are options you can enable in the Tags view.

| Option                   | Description                                    |
|--------------------------|------------------------------------------------|
| Export Files With Report | Export tagged files in the tag with the report |
| Censor Pictures          | Blur images in the tag                         |





By default, tagged files are not exported when a report is generated. To export the tagged files, mark the **Export Files With Report** checkbox.

Sometimes a case includes images that are sensitive or cannot be legally possessed by certain parties. Mark the **Censor Pictures** checkbox to blur these images. The images are visible in the Tags view, but the Report view and the report itself censors the pictures.

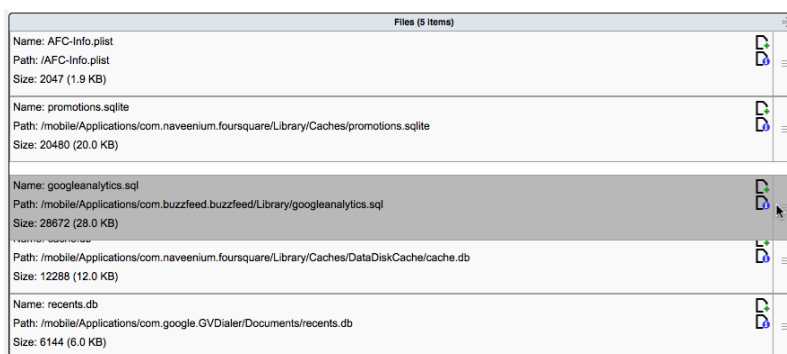
You can expand or collapse items in the Content pane create more space to view other items. By default, items are expanded. In the upper right corner of each item in the Content pane, click expand or collapse.



These are the other options for tagged items.

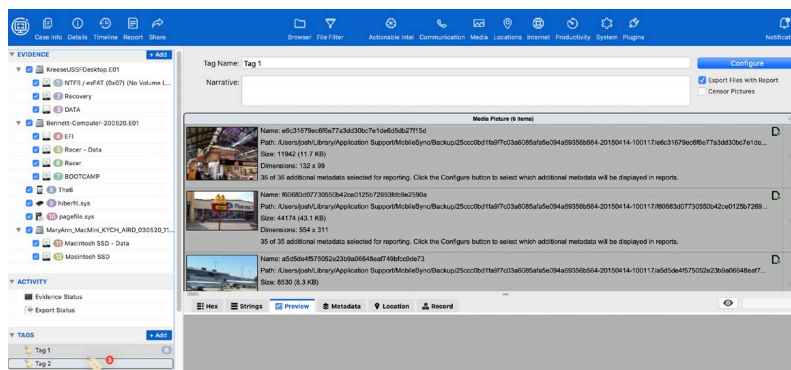
| Option                                                                            | Description                                                                                                                    |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
|  | Add a note to the selected tagged item                                                                                         |
|  | A tagged item has a note. Click to edit the note                                                                               |
|  | A tagged item has associated metadata. Click to change the metadata selections included in the examiner report                 |
|  | A tagged item has a geolocation data. Click to add the location map along with the item. The icon will turn green if selected. |

Tagged items can be rearranged within a tag. Tagged items closer to the top of the list appear earlier in the examiner report. On the far right of the tagged item is a handle. Grab and hold the handle and drag the item up or down to move it in the list. Release the item in the appropriate position in the list.



You can move tagged items to other tags by dragging and dropping. Select a tagged item or multiple tagged items and drag them to another tag. A red number badge appears indicating the number of tagged items being moved if more than one item is selected.

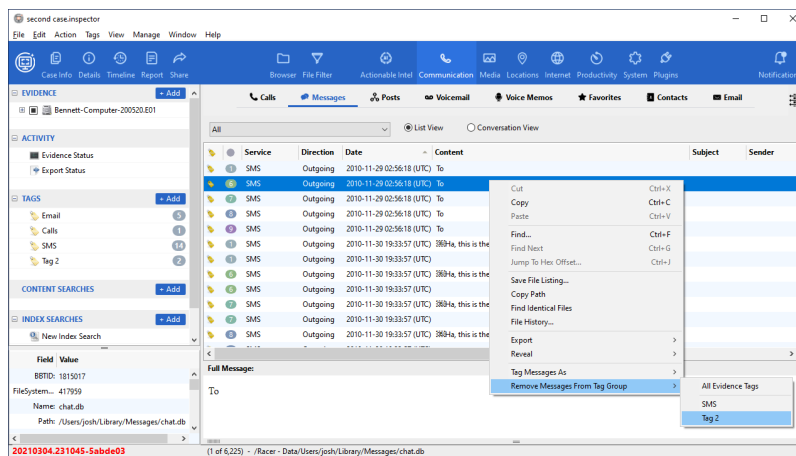
When items are moved to a tag in the Component list, a gray border appears around the destination tag name. When the items are moved to the correct destination tag, drop the items. The number badges for both the source and destination tags reflect their new tagged item count.



## Deleting Tags

Items can be removed from tags, and the tags themselves can be deleted. Open the context menu for a tag or a tagged item to see the menu options.

For tagged items in any view, the menu shows every tag container that item is stored in and allows removal from all or some of the containers.



In the Tags view, you can remove an item from a tag. Select the item and press **DELETE**, or in the menu bar click **Tags > Delete Selected Tag Item**.

In the Tags view, you can remove all tagged items from a tag but keep the tag itself. Select all the items in the tag and press **DELETE**.

In the Tags view, you can delete a tag and remove all items in that tag from the case. Select the tag in the Tags view and press **DELETE**, or in the menu bar click **Tags > Delete Selected Tag**.

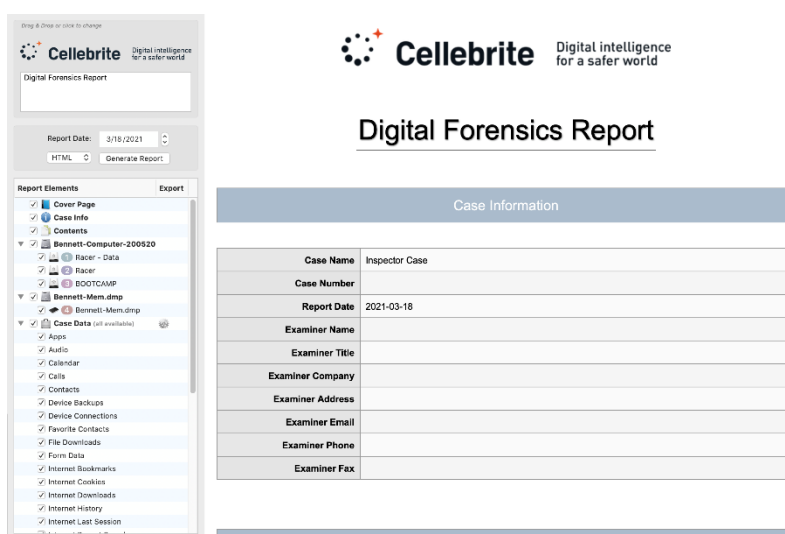
# Reporting

This chapter provides these topics about reporting in Inspector.

- [Report View](#)
- [Tags and Tagged Items](#)
- [Reporting Device Details](#)
- [Generating and Exporting the Examiner Report](#)

## Report View

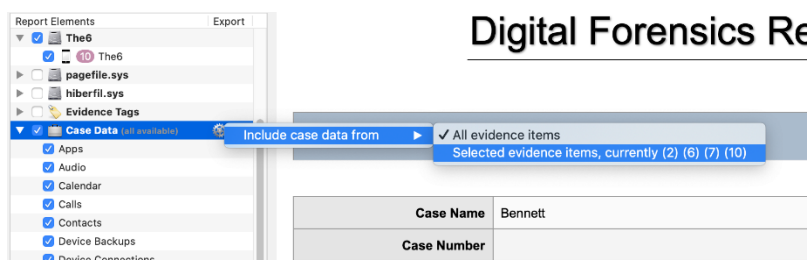
In the toolbar, click **Report**. Options for the examiner report appear along with a report preview.



You can create a simple report that details all of the information without first tagging everything in the case. In the report side bar, click **Case Data** in the Report Elements section. This lets you quickly select everything or select only certain things to report on. To select all or none, press SHIFT while you click on the report element header.

You can customize the report logo by dragging and dropping a new logo on top of the Cellebrite logo. Alternatively, you can click the logo to select a new one.

You can select evidence items to report on, then click **Configuration** (the wheel icon) to the right of Case Data. Choose **Selected evidence items** from the menu, and only those items will appear in the report.



HTML reports are broken down into smaller pages to make it easier to load into web browsers.

Items in the Report Elements list correspond to items in the Case Info view, and the Evidence and Tags sections of the Component list. You can include a table of contents that links to each section of the report. The Contents section links works in reports exported to .html, .pdf, or .docx format.

To include or exclude Report Element items from the examiner report, mark or unmark the checkbox to the left of each item. To change the order of items in the Report Elements list, select and drag the items up or down and release them in the appropriate location. Report elements appear in the examiner report in the order that they are listed; elements at the top of the list appear first in the examiner report. Move important elements or evidence to the top of the list to include them earlier in the report.

## Tags and Tagged Items

Select and drag the tags up and down to change the order in which tags and tagged items appear in the examiner report. While you can reorder tags in the Report view, individual tagged items within each tag cannot be reordered in this view.

To reorder individual items within a tag, in the Tags section of the Component list, select the appropriate tag. On the right side of each tagged item, click and hold the handle (three gray horizontal hash marks), drag the item up or down, and release it in the appropriate location. To see the item's new location in the report in the examiner report preview, click **Report** in the toolbar. For more information, see [Tags](#).

To see both the Tags section and the Report view at the same time, on the menu bar click **Window > New Window for this Case**. Place the two windows side by side. Select a tag in one window, and on the toolbar in the other window, click **Report**. In the Tags window, select a tag and reorder the items within the tag. In toolbar of the Report window, click **Report** to refresh the report preview. Tagged items appear in their new order in the report.

## Reporting Device Details

You can show or hide data associated with each device listed in the Report Elements section. Note that disk image partitions and unallocated space are listed separately in the Report Elements list, and a checkbox appears to the left of each. Conversely, each device representing a logical acquisition, such as an evidence folder or an iOS device backup, normally has only one data item with one checkbox associated with it.

The screenshot displays the Cellebrite Inspector Cloud interface. The main pane shows the details for 'Device: The6 -- (Evidence ID: The6 - 001)'. The 'Report Elements' section on the left lists various data items with checkboxes for inclusion or exclusion in the report. The 'Details' pane on the right provides specific information about the device, including its path, type, sector size, and various attributes like name, snapshot date, model version, carrier, capacity, phone number, cellular usage, data available, data used, OS version, product type, and model number.

| Device: The6 -- (Evidence ID: The6 - 001) |                                                                                                                                  |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Path                                      | /Users/owner/Desktop/Inspector Case Inspector/Partitions/A71365073F692E5F4AE14680AF98A401/A71365073F692E5F4AE14680AF98A401/Files |
| Type                                      | iOSBackupEncrypted                                                                                                               |
| Sector Size                               | 512                                                                                                                              |
| Initial Report Writer Case Version        | Inspector 10.3                                                                                                                   |
| Name                                      | The6                                                                                                                             |
| Snapshot                                  | Not Available                                                                                                                    |
| Snapshot Date                             | Not Available                                                                                                                    |
| Model Version                             | iPhone 8 (Model A1863, A1905, A1908, A1907)                                                                                      |
| Carrier                                   | Not Available                                                                                                                    |
| Capacity                                  | Not Available                                                                                                                    |
| Phone Number                              | (240) 494-6399                                                                                                                   |
| Cellular Usage                            | +14083340585, +16475839559, +12404946399                                                                                         |
| Data Available                            | Not Available                                                                                                                    |
| Data Used                                 | Not Available                                                                                                                    |
| OS Version                                | 13.3                                                                                                                             |
| Product Type                              | iPhone10,1                                                                                                                       |
| Model Number                              | Not Available                                                                                                                    |

To include or exclude device details in the Details view of the report for any partition, either mark or unmark the checkbox for any partition in the Report Elements section.

Device details from the Details view cannot be included or excluded individually via the Inspector Report view. However, these items are exported separately. Therefore, you may delete them as necessary after the report is generated and exported.



## Generating and Exporting the Examiner Report

In the top left corner of the Content pane, set the Report Date to the current date, and then select an export file format for the report. Examiner reports can be exported as searchable .pdf, .html, .docx, .csv, or plain text files.

**Note:** Natively rendered chat histories (graphic representations) are also searchable.

To preview the report prior to export, drag the scroll bar on the right side of the Content Pane up or down (using the scroll bar navigation arrows at the bottom of the scroll bar).

For email previews to be included in reports, you must enable them on the Reports tab of the Preferences or Options window for Inspector. For more information, see [Inspector Preferences or Options](#). Additionally, the emails must be tagged either within the Email sub-view of the Communications view or from Index Search when the **Type** field is **Email**, and you must also mark the **Export** checkbox in the Report view.

After all settings are set as desired, click **Generate Report**. A Save prompt appears.

Inspector exports the examiner report to a folder with the default name *Inspector Report <current date and timestamp>*. To change the default folder name, type a new folder name into the **Save As** field. Choose a location to save the report and click **Save**.

When the report generator finishes creating the report, a Report Complete dialog box appears. To see the exported report in the file system, click **Reveal Report**. To open the report, click **Open Report**. You may view, search, and modify the exported report in an appropriate application, such as Microsoft Word (.docx report) or a web browser (.html report). The report folder contains the report itself and an Evidence folder. The Evidence folder contains exported files associated with tags where the Export checkbox within the Report Elements list was checked. The Evidence folder also contains an *\_\_Export Log.txt* file.

## Portable Cases

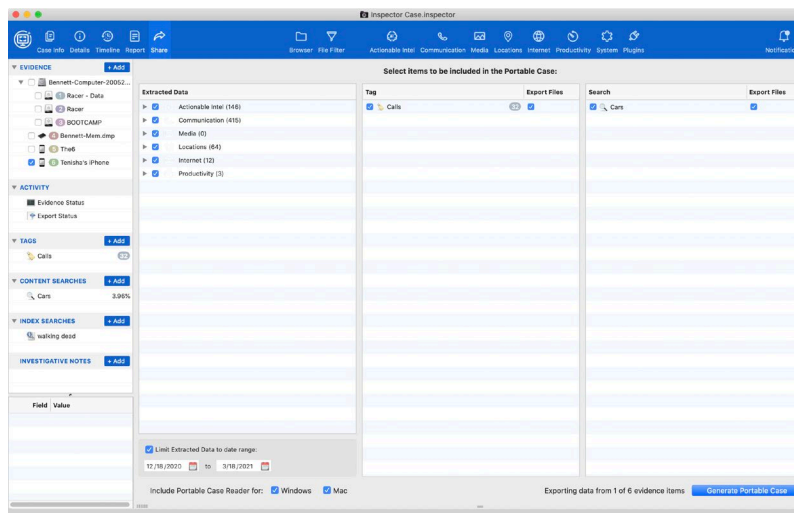
This chapter provides these topics about portable cases in Inspector.

- [Select Data for the Portable Case](#)
- [Generating and Reviewing a Portable Case](#)
- [Portable Case Interface](#)

## Select Data for the Portable Case

Inspector's Portable Case feature lets you share case data for offline review. A portable case does not rely on access to the original evidence files. Instead, logical evidence files are created. These include only data selected for sharing as part of the portable case file.

To create a portable case file, click **Share** on the toolbar. From the evidence items parsed listed in the Component list, select the evidence to include in the portable case. The Content pane contains these areas: Extracted Data, Tag, and Search. By default, all data in each area is selected for inclusion.



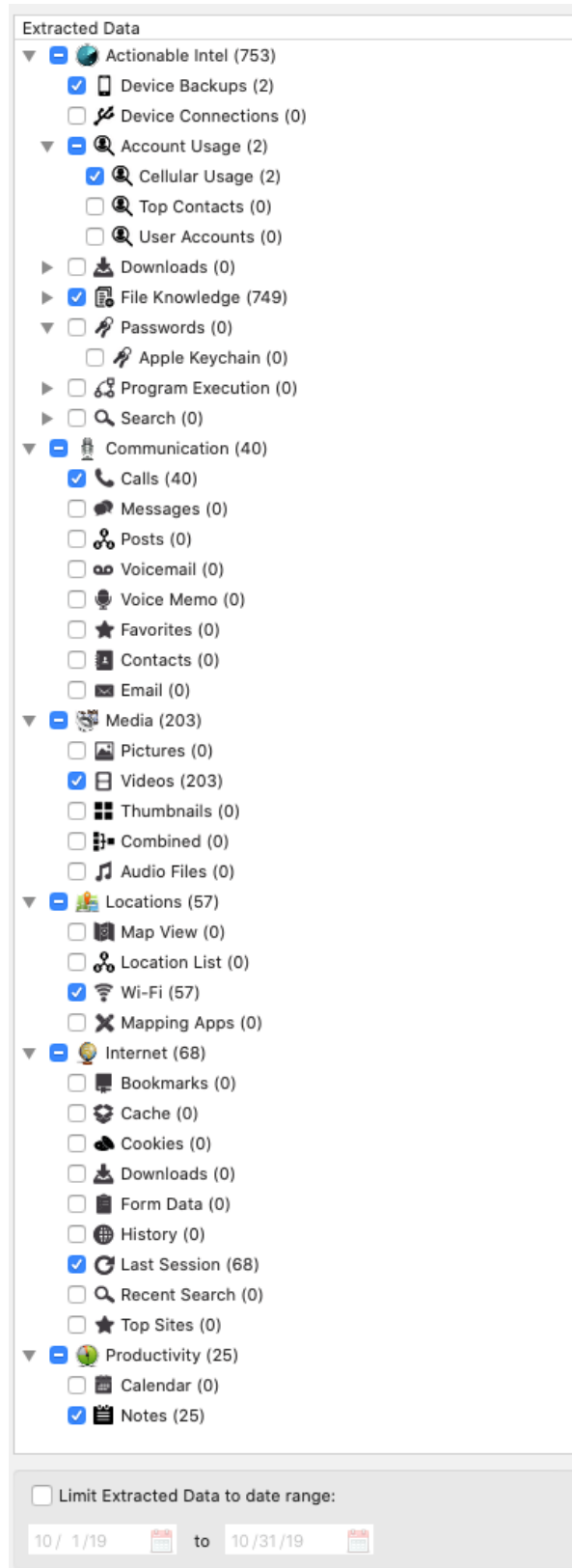
## Extracted Data

In Extracted Data, sections of Inspector where data is parsed are listed, including Actionable Intel, Communications, Media, Locations, Internet, and Productivity. For each section, the associated processing options must be run for data to be parsed. For example, if Video Analysis has not been run, no Videos will be listed for extraction in the Media section. In parentheses after each section label, the number of items parsed for that label is listed. If the number of items for a section is listed as (0), either no data of that type was parsed from evidence or the processing option to parse that data has not been run. As items are selected or deselected in the Component list these numbers automatically adjust.

For each Extracted Data type selected, the associated files are exported into a logical evidence file for inclusion in the portable case. For some Extracted Data types, such as Media, the number of files and the size of the files for an evidence item can be quite large. Keep this in mind while you choose data to include in portable cases.

You can show or hide sub-views parsed for each type of Extracted Data type. Some sub-views, like Downloads in Actionable Intel, have additional sub-views. To exclude an Extracted Data type from the portable case, unmark the checkbox for that data type.

At the bottom of Extracted Data, you can mark the checkbox for **Limit Extracted Data to date range**. Do this to limit the data included in the portable case to a time period of interest to the reviewer. Limiting the data based on a date range may be useful in cases where the reviewer is only allowed to see items from a specific period of time. With this enabled, the number of items for each Extracted Data section is adjusted to show the number of items that fall within the specified date range.



## Tags

All tags the examiner created in the case files appear in the Tag section. The name of the tag appears with the number of items included in the tag. Just like creating a Report in Inspector, there is an option to Export Files for each tag. When this option is chosen, the files associated with the tagged data are export into the portable case, stored in a logical evidence file. Tagged data overrides any date range specified in Extracted Data. Tags selected are included in the portable case even if the tagged data does not fall within the specified date range.

## Search

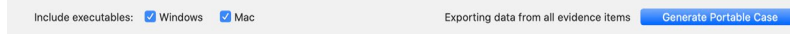
The Search section in the Share view lists the content searches that were performed. Content searches locate data based on keywords. This mechanism can be used to effectively limit the data in the portable case based on keywords of interest to the reviewer. While content searches cannot be limited by a date range in the Share view, data can be filtered when running a content search by date.

The screenshot displays the Search configuration interface. On the left, a filter criteria section shows a tree view with 'Any' selected. Below it, four criteria are listed: 'Date Created', 'Date Modified', 'Date Added', and 'Date Accessed'. Each criterion is set to 'is between' with a date range of '1/ 1/2019' and '12/30/2019'. On the right, the 'Options' section includes a 'Search:' dropdown set to 'Content only', checkboxes for 'Case Sensitive', 'Unicode (UTF16)', 'Deep Search', and 'Skip Files Larger Than:' (set to 2 GB), and a checkbox for 'Report Only First Hit on File'. A red box highlights the 'Files that Match Filter' dropdown, which is currently set to 'Current Unsaved Filter'. Below this, the 'Regular Expression Keyword' section includes an 'Add Preset:' dropdown and checkboxes for 'Selected Keyword is RegEx Pattern' and 'Add Word Bounding to Pattern'.

Content searches selected for inclusion are available in the portable case.

## Generating and Reviewing a Portable Case

Once items have been selected to be included in the portable case, you can choose which Inspector Portable Case readers will be exported with the portable case data. By default, Portable Case readers for both Windows and Mac computers are selected. Leave them both selected if you don't know exactly which platform will be used to review the case. Click **Generate Portable Case**.



If indexing was run on the evidence items selected for export, a new index will be created containing only the evidence items that fit the criteria for inclusion. The default name of the portable case file is taken from the name of the Inspector case file. When one or more reader is included, a folder is created for the portable case which contains the portable case file and the readers. The folder name matches the portable case name.

Once portable case generation begins, the bottom of the Content pane shows the status. The data is prepared and then exported into a .PortableCase file. Like an Inspector case file, on Mac computers the .PortableCase file is a bundle that contains files and folders. The .PortableCase file is created in a folder along with the selected readers in a compressed format. If no readers were included, only the .PortableCase file is created. This example shows portable cases created with both readers included, one reader included, and no reader included.

| Name                           | Size     | Kind          |
|--------------------------------|----------|---------------|
| ▼ Bennett                      | --       | Folder        |
| Bennett.PortableCase           | 28.32 GB | Portable Case |
| Portable Case 10.1_macOS64.zip | 1.08 GB  | ZIP archive   |
| Portable Case 10.1_win64.zip   | 1.17 GB  | ZIP archive   |
| ▼ Search                       | --       | Folder        |
| Portable Case 10.1_win64.zip   | 1.17 GB  | ZIP archive   |
| Search.PortableCase            | 27.48 GB | Portable Case |
| Tag.PortableCase               | 255.9 MB | Portable Case |

The size of the portable case depends on what data was included in the export.

## Reviewing a Portable Case

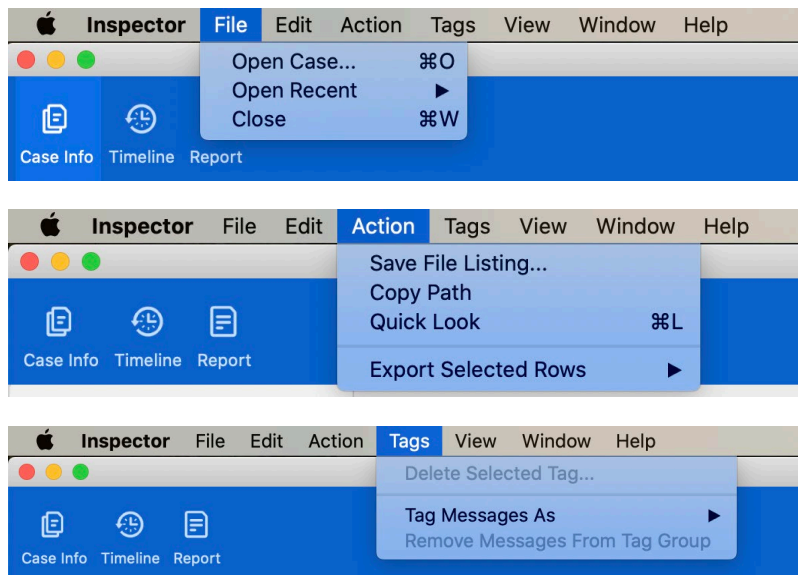
Once a portable case is created, you should open it with Inspector to review the contents and ensure the appropriate data was included. If any information was missed when the portable case was generated, you must create a new portable case. Data cannot be added to a portable case file.

## Portable Case Interface

The Inspector Portable Case reader resembles Inspector. When you open a portable case file with Inspector, some functions of Inspector are disabled, in effect creating an experience similar to the Portable Case reader.






### Menu Bar

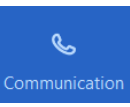

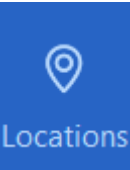

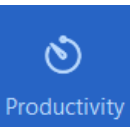
Options in the menu bar provide access to limited functions. From the menu bar, you can open and close cases, save file listings, export selected rows (in tab-delimited or csv format), and perform tagging functions.



## Toolbar

The toolbar is used to select the view to show in the Content pane. Some buttons always appear. Other buttons appear only if data corresponding to them was selected or if tags were exported when the portable case was generated. For each data category selected, the corresponding button appears. If a portable case contains data only from exported tags and none from Extracted Data, the icons correspond to the data contained in the exported tags (with one exception).

| Button                                                                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br><b>Case Info</b>          | <p>See case details, including Examiner Information, Case Information and Case Time Zone Display.</p> <p>You may change the Case Time Zone Display.</p> <p>Always appears.</p>                                                                                                                                                                                                                                                                                                   |
| <br><b>Report</b>             | <p>See the examiner report.</p> <p>You can generate new reports containing information identified during the review process.</p> <p>Always appears.</p>                                                                                                                                                                                                                                                                                                                          |
| <br><b>Browser</b>           | <p>See the files included in the portable case, stored in the same structure as the original file system.</p> <p>You can navigate through the file structure containing the exported files. You can see file timestamps, sizes, extensions, and hash values. You can select a column heading to sort files by the column attribute.</p> <p>Always appears.</p>                                                                                                                   |
| <br><b>File Filter</b>      | <p>See the file filters from Inspector.</p> <p>While all file filters are listed, they do not all work. Portable cases maintain limited metadata. For example, geolocation metadata is not stored in portable case. The built-in saved filter Geo Location is still available in portable cases, but running it returns no results. The File Information pane topic lists available metadata. For more information, see <a href="#">File Filters</a>.</p> <p>Always appears.</p> |
| <br><b>Actionable Intel</b> | <p>See various types of data that can mostly be attributed to a user's actions. The data is stored in a tree style menu with sub-views of these items.</p> <ul style="list-style-type: none"> <li>• Device Backups</li> <li>• Device Connections</li> <li>• Account Usage</li> <li>• Downloads</li> <li>• File Knowledge</li> <li>• Passwords</li> <li>• Program Execution</li> <li>• Search</li> </ul>                                                                          |

| Button                                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  Communication  | See sub-views containing calls, messages, posts, voicemail, voice memos, favorites, contacts, and email. This includes data parsed from SMS, iMessage, and messages from other communication apps such as Skype, WhatsApp, Textfree, Kik, and so forth.                                                                                                                                                                                            |
|  Media          | See sub-views containing Pictures, Videos, or Thumbnails, or use the Combined sub-view to see all these together. The Videos sub-view includes the 4 x 4 mosaics made up of sixteen frame-sequence slices. The Audio sub-view lets you see and play audio files.<br><br>This view is available only when Media is selected in the Extracted Data section during case generation. Tagged media does not populate the Media view in a portable case. |
|  Locations      | See this data. <ul style="list-style-type: none"> <li>• Google and Apple Maps usage</li> <li>• geolocation data from media files, calendar and social media apps</li> <li>• Wi-Fi network information</li> <li>• additional location services data</li> </ul>                                                                                                                                                                                      |
|  Internet      | See internet history and cache information for Safari, Firefox, Chrome, Internet Explorer, and Edge browsers.<br><br>The Internet view displays exported information associated with Safari, Firefox, Google Chrome, Internet Explorer, and Edge web browsers.                                                                                                                                                                                     |
|  Productivity | See data from the Calendar and Notes applications (macOS and iOS).                                                                                                                                                                                                                                                                                                                                                                                 |

Exported search items do not affect the views available in the toolbar. Data included in the portable case by means of a content search is accessible in the Browser and File Filter views.

## Component List

The Component list includes these sections.

- Evidence
- Content Searches
- Index Searches
- Tags
- Investigative Notes

Just as with Inspector, the Evidence section of the Component list contains a hierarchical device list. Only evidence items selected when the portable case file was created are listed. The original badge numbering from Inspector file transfers to the portable case. In a portable case, evidence items can be reordered by highlighting a specific item and dragging it up and down in the list. New evidence items cannot be added to the portable case. To review the data in the devices or device partitions, they must be selected in the Evidence section.

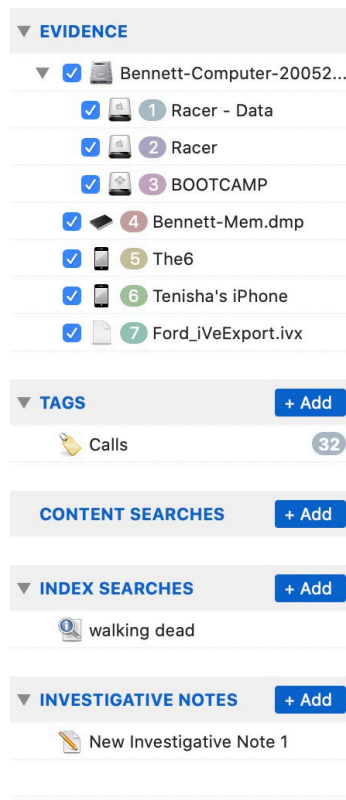


The Tags section of the Component list provides access to Tag data included in the portable case. Tags exported during portable case generation cannot be altered. The case reviewer can create, edit and delete new tags in the portable case.

The Content Searches section of the Component list allows users to create content searches and displays content searches exported into the portable case. Any new content searches are saved in the portable case file. To create a new content search, click **Add**. For more information, see [Search](#).

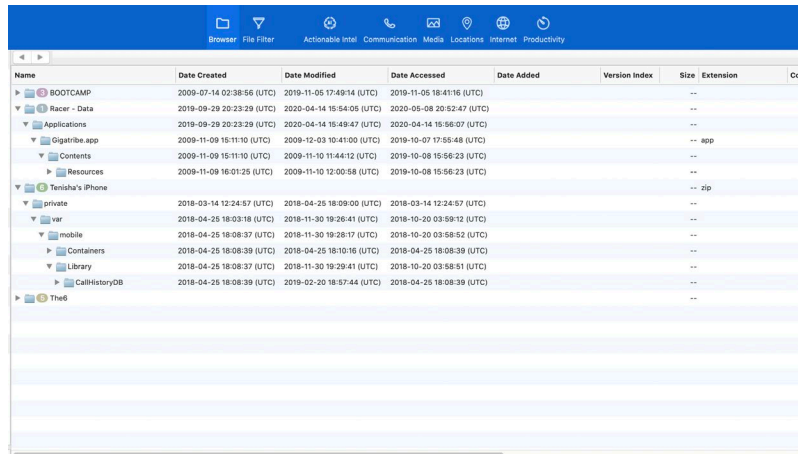
The Index Searches section of the Component list provides access to the Smart Index. If the exported data was indexed in the Inspector case, the portable case will contain a Smart Index. Queries of the Smart Index are saved in the portable case file. To create a new Index Search, click **Add**. For more information, see [Search](#).

The Investigative Notes section of the Component list provides an area for the case reviewer to copy and paste or type in information they wish to note during the case review. To create a new Investigative Note, click **Add**.



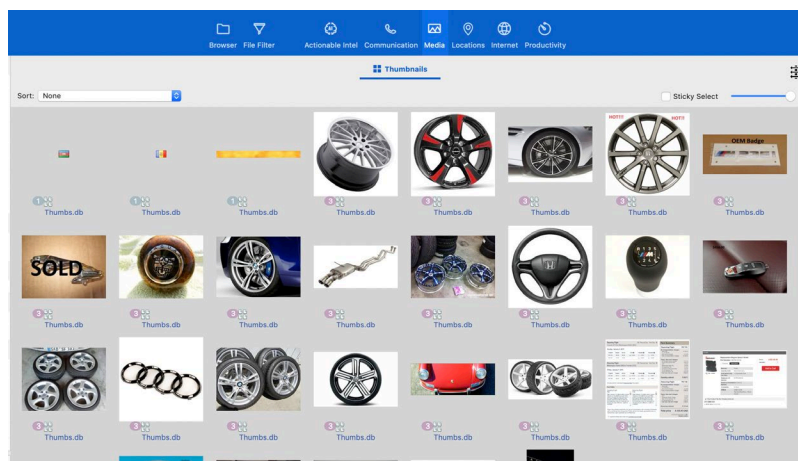
## Content Pane

Information displayed in the Content pane depends on the view selected in the toolbar and the devices selected in the Evidence section of the Component list. This example shows the Browser view.



| Name             | Date Created              | Date Modified             | Date Accessed             | Date Added | Version Index | Size | Extension | Cont |
|------------------|---------------------------|---------------------------|---------------------------|------------|---------------|------|-----------|------|
| BOOTCAMP         | 2009-07-14 02:38:56 (UTC) | 2019-11-05 17:49:14 (UTC) | 2019-11-05 18:41:16 (UTC) |            |               |      |           |      |
| Racer - Data     | 2019-09-29 20:23:29 (UTC) | 2020-04-14 15:54:05 (UTC) | 2020-05-08 20:52:47 (UTC) |            |               |      |           |      |
| Applications     | 2019-09-29 20:23:29 (UTC) | 2020-04-14 15:49:47 (UTC) | 2020-04-14 15:56:07 (UTC) |            |               |      |           |      |
| Gigabyte.app     | 2009-11-09 15:11:10 (UTC) | 2009-12-03 10:41:00 (UTC) | 2019-10-07 17:55:48 (UTC) |            |               |      | app       |      |
| Contents         | 2009-11-09 15:11:10 (UTC) | 2009-11-10 11:44:12 (UTC) | 2019-10-08 15:56:23 (UTC) |            |               |      |           |      |
| Resources        | 2009-11-09 16:01:25 (UTC) | 2009-11-10 12:00:58 (UTC) | 2019-10-08 15:56:23 (UTC) |            |               |      |           |      |
| Tenisha's iPhone |                           |                           |                           |            |               |      | zip       |      |
| private          | 2018-03-14 12:24:57 (UTC) | 2018-04-25 18:09:00 (UTC) | 2018-03-14 12:24:57 (UTC) |            |               |      |           |      |
| var              | 2018-04-25 18:03:18 (UTC) | 2018-11-30 19:26:41 (UTC) | 2018-10-20 03:59:12 (UTC) |            |               |      |           |      |
| mobile           | 2018-04-25 18:08:37 (UTC) | 2018-11-30 19:28:17 (UTC) | 2018-10-20 03:58:52 (UTC) |            |               |      |           |      |
| Containers       | 2018-04-25 18:08:39 (UTC) | 2018-04-25 18:10:10 (UTC) | 2018-04-25 18:08:39 (UTC) |            |               |      |           |      |
| Library          | 2018-04-25 18:08:37 (UTC) | 2018-11-30 19:29:41 (UTC) | 2018-10-20 03:58:51 (UTC) |            |               |      |           |      |
| CallHistoryDB    | 2018-04-25 18:08:39 (UTC) | 2019-02-20 18:57:44 (UTC) | 2018-04-25 18:08:39 (UTC) |            |               |      |           |      |
| The6             |                           |                           |                           |            |               |      |           |      |

This example shows the Thumbnails sub-view in the Media view.



The views for Actionable Intel, Communication, Media, Locations, Internet, and Productivity have a file filter. To show or hide the file filter, click **Show/Hide Filter** (three arrows) at the top right of the Content pane. When the **Show/Hide Filter** button is black, no filter is applied. While at least one filter is applied, the button is green.

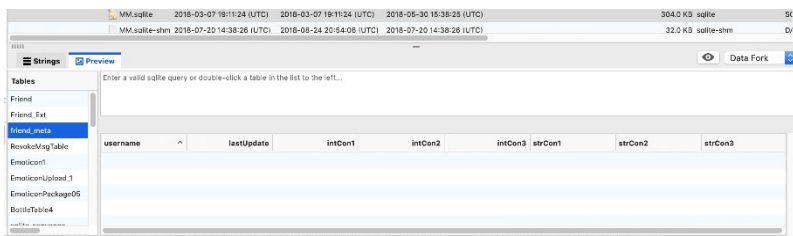
## File Content View

With a file selected in the Content pane, the File Content view provides two options to see the selected item, Strings or Preview.

To see ASCII printable strings of three characters or more, click **Strings**.

To see a file as it would appear in its native application, click **Preview**.

If the selected file is a text file, you can perform a keyword search within the displayed text strings in both the Strings view and Preview views.



Only on Mac computers, you can see the file using Quick Look. In the Content pane, select a file and then in the File Content view, click **Quick Look** (eye button). Quick Look shows native Apple application files (and some third-party application files) the same way a user sees them. Audio and video files play within Quick Look as well.

**Note:** Quick Look works only when a Quick Look plug-in for the selected file type, or an application that supports the selected file type, is installed on the examiner's computer.

## File Information Pane

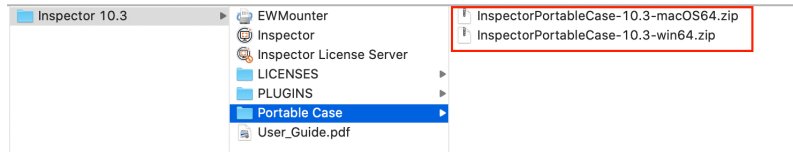
The File Information pane shows metadata associated with a file selected in the Content pane. In a portable case file, the shown metadata is limited to common file system metadata, some filesystem metadata unique to APFS and HFS+, and some metadata stored for the file from Inspector processing. These fields are available for files in the File Information pane:

- BBTID - The reference ID of a given file or folder within Inspector's casefile database
- FileSystemID - The filesystem ID parsed from the file record
- Name
- Path
- Size - Logical size
- SizeOnDisk
- Extension - File extension stored in file system
- Content Extension - Displays the extension based on content header (file signature)
- Date Created
- Date Changed
- Date Modified
- Date Accessed
- FileSystemOffset
- fsType
- Directory
- Visible - Displays hidden/visible status
- Locked - Displays locked/unlocked status (e.g., read-only)
- Owner ID (macOS, iOS)
- Group ID (macOS, iOS)
- Permissions (macOS, iOS)
- Entropy
- ForkCount
- MD5
- SHA1
- SHA256

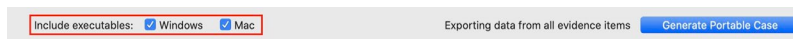
**Note:** Metadata for directories differs from file metadata.

## Accessing Portable Case Files

When you install Inspector, you are provided with .zip files containing the portable case readers for Mac and Windows computers.



When the checkboxes for including the executables for Windows and Mac are marked, these .zip files are copied into the folder created for the portable case when it is generated.



The case reviewer should decompress the .zip file for the version of the Portable Case reader appropriate for the platform of their reviewing computer.

Inspector Portable Case readers cannot open Inspector case files, do not require installation, and do not require an Inspector license.

## Hash Set and File Signature DB Management

This chapter provides these topics about hash set and file signature database management for Inspector.

- [Hash Sets](#)
- [File Signature Databases](#)
- [PhotoDNA and Project VIC](#)
- [C4All](#)
- [Semantics21](#)

### Hash Sets

Cellebrite provides hash sets for use in Inspector from our website. The hash sets include a Known OS X System Files hash set and a Known Windows System Files hash set. The Known OS X System Files hash set includes MD5 hashes for every system file from OS X 10.0.0 through OS X 10.15.7 for Intel architectures. The Known Windows System Files hash set includes MD5 hashes for Windows version 7, 7.1, 8, 8.1, and 10.

All hash set databases include only unique file hashes.

By default, hash sets are saved in the */Application Support/Cellebrite/Hash Sets* folder. This folder is found in these locations, depending on the operating system of the analysis computer.

- macOS: */Users/<username>/Library/Application Support/Cellebrite/Inspector/Hash Sets*
- Windows 10: *C:\Users\<username>\AppData\Roaming\Cellebrite\Inspector\Hash Sets*

You may also import existing custom Inspector (.blhs), EnCase (6.19 and lower), and NSRL hash sets. Hash sets saved as plain text documents may be imported, as long as the document contains one hash value per line with each line separated by a carriage return. Hashes contained in a plain text document can be MD5, SHA-1, or SHA-256. Inspector automatically identifies the hash type when the file is imported. Custom hash sets created in Inspector are automatically saved in the .blhs format and are available for use in all Inspector cases.

To view and manage hash sets in Inspector, in the menu bar click **Manage > Hash Sets**.

There are two ways you can add an Inspector .blhs format hash set.

- In the bottom left corner of the Manage Hash Sets window, click **Import** and navigate to and select the desired hash set.
- From Finder on Mac computers or File Explorer on Windows computers, drag a hash set onto the Manage Hash Sets window.

You cannot remove bundled Inspector hash sets; however, you can remove custom hash sets created using Inspector or imported hash sets.

- To remove a hash set, select a hash set in the list, and in the bottom left corner of the Manage Hash Sets window click **Remove**.

You can import an Encase, NSRL, or text file hash set.

- In the bottom corner of the Manage Hash Sets window, click **Import**. Navigate to and select the hash set, and then click **Open**.

You can generate and save a custom hash set from specific files in any Inspector view.

1. Select the files of interest either manually, by running a filter, or by selecting all files in the case.

To generate a hash set of every file in a case, open the Browser view, and then select the root folder (at the top of the file list).

2. In the menu bar, click **Action > Export Hash Set**.
3. In the Hash Set Export window, select which hash values to store in the hash set, and then click **Continue**.

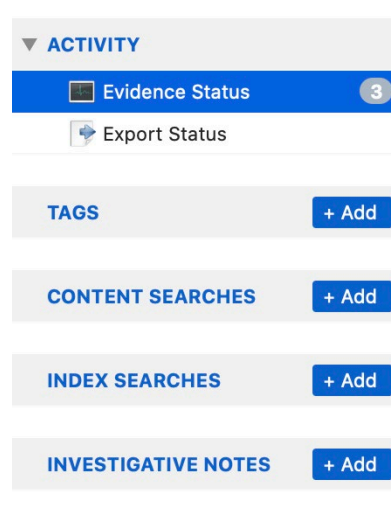


4. Type the name of the hash set, then click **Save**.

Before you run a custom hash set, you should know if the hash set contains SHA-1 or SHA-256 hash values. By default, Inspector only runs hash comparisons using MD5 hash values. You can change the Hash Comparison settings on the General tab in the Preferences window. For more information, see [Inspector Preferences or Options](#).

When this preference is set correctly, you can run this process.

1. Select **Evidence Status** in the Component list.



2. For the appropriate device, click the yellow **Play** button next to Known Files.
3. In the Hash Sets window, mark the checkbox for the custom hash set, click **OK**, and wait for processing to complete.  
The Known Files column shows Pending until the process is complete.
4. When the process is complete, select the device in the Component list, and then click **File Filter** in the toolbar.
5. In the field on the left, select **Hash Set**, then choose either **Files In Hash Set** and **Files Not In Hash Set** in the middle field.
6. In the field on the right, select the custom hash set by name, and then click **Filter**.

You can repeat this process on multiple devices and compare the results.

You can rerun a hash set even if it shows as complete in the Hash Sets window.

1. On a hash set is shown as Complete, open the context menu and click **Rerun**.
2. Now you can mark the checkbox for that hash set and run the hash set again.

| All                                                                                                                                                                        |        |                  |           |                                  |                           |                           |                           |         |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|------------------|-----------|----------------------------------|---------------------------|---------------------------|---------------------------|---------|--|
| Hash Set                                                                                                                                                                   |        | Files In Hash... |           | Known Windows System Fil...      |                           | + condition + (group)     |                           |         |  |
| <input type="checkbox"/> Invert Filter <input type="checkbox"/> Ignore Folders and Duplicate Files <span>Reset...</span> <span>Save This Filter</span> <span>Filter</span> |        |                  |           |                                  |                           |                           |                           |         |  |
| BL ID                                                                                                                                                                      | FS ID  | Name             | Size      | MD5                              | Date Created              | Date Modified             | Date Accessed             | Date Ac |  |
| 392                                                                                                                                                                        | 28     | \$Repair         | 9.0 MB    | D4108CD98F008204E9800998ECF8...  | 2018-12-17 17:05:48 (UTC) | 2018-12-17 17:05:48 (UTC) | 2018-12-17 17:05:48 (UTC) |         |  |
| 787                                                                                                                                                                        | 69974  | desktop.ini      | 129 Bytes | A52689E7C71883489D8CC062F8CE...  | 2018-12-17 14:54:11 (UTC) | 2018-12-17 14:54:11 (UTC) | 2019-01-24 20:15:07 (UTC) |         |  |
| 759                                                                                                                                                                        | 87003  | desktop.ini      | 129 Bytes | A52689E7C71883489D8CC062F8CE...  | 2018-12-17 17:28:53 (UTC) | 2018-12-17 17:28:53 (UTC) | 2018-12-17 17:28:53 (UTC) |         |  |
| 776                                                                                                                                                                        | 89100  | desktop.ini      | 129 Bytes | A52689E7C71883489D8CC062F8CE...  | 2018-12-17 14:02:31 (UTC) | 2018-12-17 14:02:31 (UTC) | 2019-01-25 18:07:56 (UTC) |         |  |
| 779                                                                                                                                                                        | 169414 | desktop.ini      | 129 Bytes | A52689E7C71883489D8CC062F8CE...  | 2019-01-25 16:31:22 (UTC) | 2019-01-25 16:31:22 (UTC) | 2019-01-25 16:35:06 (UTC) |         |  |
| 817                                                                                                                                                                        | 162022 | msvcp120.dll     | 644.7 KB  | 46060C35F6972818C5E737AE372...   | 2019-01-25 16:37:43 (UTC) | 2019-01-25 16:37:43 (UTC) | 2019-01-25 17:04:02 (UTC) |         |  |
| 818                                                                                                                                                                        | 162036 | msvcrt20.dll     | 940.7 KB  | 9C861C079D08176286C54E3769787... | 2019-01-25 16:37:43 (UTC) | 2019-01-25 16:37:43 (UTC) | 2019-01-25 17:04:02 (UTC) |         |  |
| 1883                                                                                                                                                                       | 20996  | ipid.xml         | 2.5 KB    | 421880588B869696027618E7869F...  | 2018-04-11 23:35:07 (UTC) | 2018-04-11 23:35:07 (UTC) | 2018-04-11 23:35:07 (UTC) |         |  |
| 1885                                                                                                                                                                       | 21018  | Alphabet.xml     | 772.9 KB  | 6176656C4D6A2158D670D58D63D3...  | 2018-04-11 23:35:07 (UTC) | 2018-04-12 09:20:29 (UTC) | 2018-04-12 09:20:29 (UTC) |         |  |

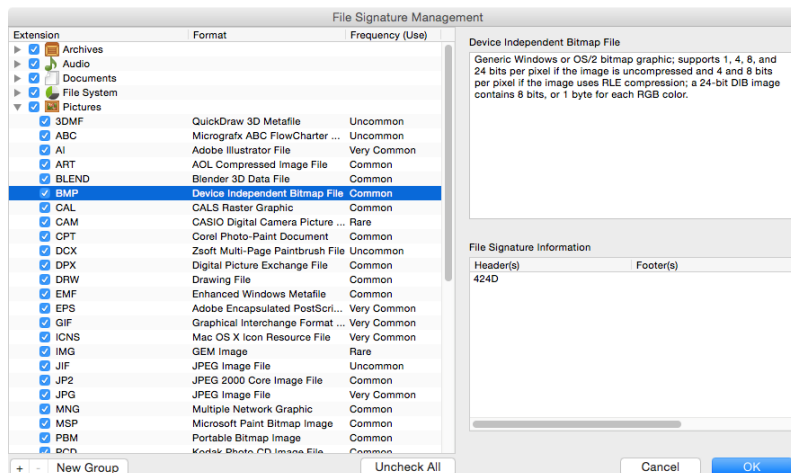
## File Signature Databases

You may create custom file signature databases and apply them during unallocated processing. By default, custom signature databases are stored as SQLite files in these locations.

- on macOS: `~/Library/Application Support/Cellebrite/Inspector/UASignatureDBs`
- on Windows: `/Users/<username>/AppData/Roaming/Cellebrite/Inspector/UASignatureDBs`

**Note:** Back up all user-defined file signature databases to a second location to preserve them for later use.

1. To create, add or remove a custom signature database, in the menu bar click **Manage > File Signatures**.
2. In the File Signature Management window appears, expand each category to see extensions for each category.
3. Select an extension from the list, and the panes at right show a description and file signature information for the extension.



To create a new file signature database, in the bottom left corner of the File Signature Management window, click **New Group**. A new signature database with the default name `UserDefinedSignatures` appears in the database file list.

To add a new file signature to an existing database, select a user-defined database in the File Signature Management window.

1. Click **+** (**add**) in the lower left of the window, and a separate signature definition window appears.
2. Provide data in each field, then click **OK**.

To remove an existing file signature, select the signature, then and click **-** (**remove**).

You can remove a file signature database from the current case. This permanently removes the database and cannot be undone. You cannot remove a database while a processor is running.

- Select the database file in the list, and in the bottom left corner of the File Signature Management window click **-** (**remove**).



## PhotoDNA and Project VIC

Authorized law enforcement users can obtain the Project VIC robust hash set and import that into Inspector to perform PhotoDNA test comparison against case photos. Project VIC Version 2.0 is supported.

**Note:** The Project VIC robust hash set must be obtained from Project VIC.

Signup and registration are offered through ICAC Cops Portal (ICAC) (ICE) (USPIS) (FBI). You must have an account on the ICAC Portal. To request membership in Project VIC, see <https://www.icaccops.com/users/Login>. The request must be approved by the ICAC Commander or designated Federal Administrator.

Before you add the Project VIC hash set to Inspector, you must set the appropriate Project VIC country. You can do this on the Project VIC tab on the Preferences window. For more information, see [Inspector Preferences or Options](#).

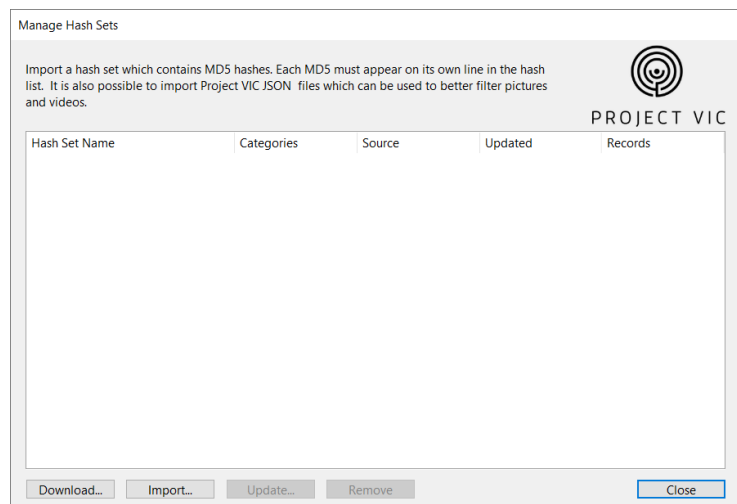
**Note:** Each set must be added individually.

### Add the Project VIC Robust Hash Set to Inspector

1. In the menu bar click **Manage > Hash Sets**.
2. Click **Import** and then select the .json file you obtained from Project VIC.  
You cannot change the name of the hash set.

When import is complete, Inspector shows how many hashes were successfully imported.

To import multiple sets, repeat this procedure. The hashes are appended to the previous entry.



If an entirely new hash set becomes available, you must remove the PhotoDNA hash set before you import the new version. Once the hashes are imported, the Manage Hash Sets window reflects the newly added PhotoDNA hash set.

When you use the PhotoDNA hash set for the first time, you must provide your password.

1. Log in to [My Cellebrite](#).
2. Click the link on the PhotoDNA Authentication dialog box to see the password, which you must enter on the PhotoDNA Authentication dialog box.

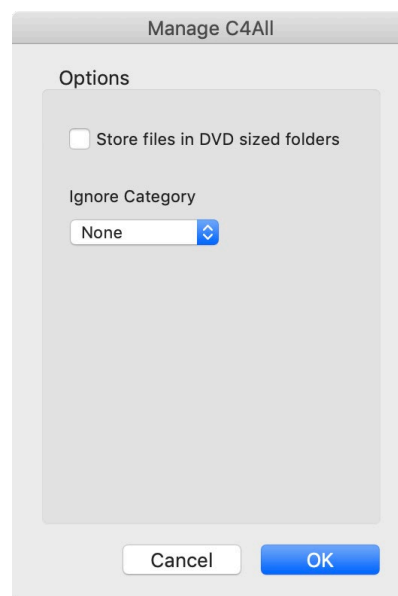
The rest of the process for running the Project VIC robust hash set against case evidence is the same as with other hash sets. For more information, see [Hash Sets](#) and [File Signature Databases](#).

## C4All

Categorizer For All, or C4All, is a tool used in the investigation of child exploitation media. Once all the necessary evidence in a case has been acquired, C4All can be used to quickly compare pictures and videos found in that evidence against an expansive database of known file hashes of child exploitation media.

Inspector has C4All fully integrated and ready to use on cases involving OS X, Windows, iOS, and Android devices. Users can connect to a locally stored C4All database in MySQL format, or one that is remotely stored with SQL Server. (To access a C4All database stored on SQL Server using a Mac computer, an ODBC driver shipped with the Inspector installer is installed automatically when Inspector is installed.)

To log into the C4All database, from the menu bar click **Manage > C4All**.



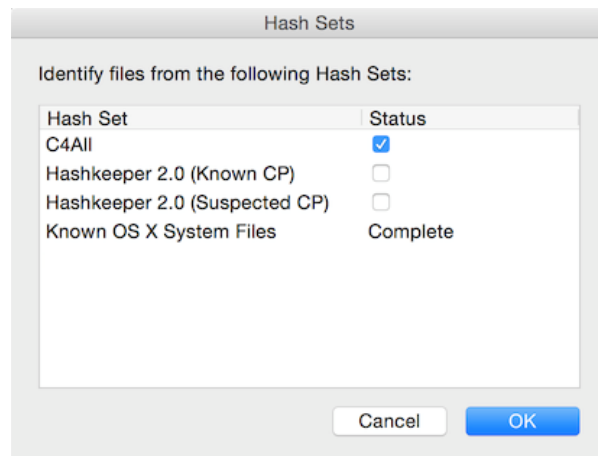
In the C4All window, you can set whether to allow the images and videos to be exported from the case file into folders that are DVD-sized. Mark or unmark the checkbox for **Store files in DVD sized folders**.

You may also choose whether a specific category of images or videos will be excluded from the export. In the **Ignore Category** field, select a category number or leave it set to None.

The settings in the Manage C4All window apply to every case for this computer.

If there are multiple evidence devices (allocated or carved files), you must run C4All against each device separately.

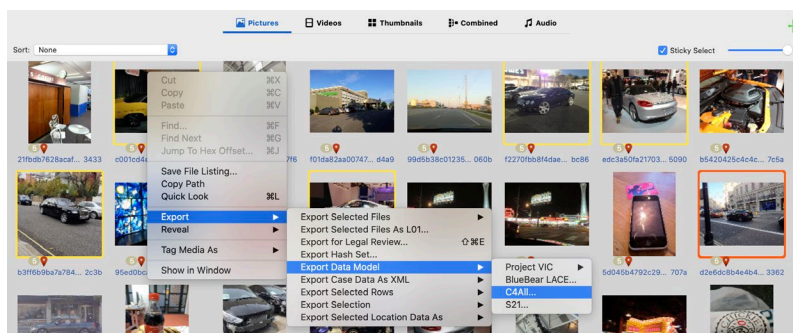
1. On the Media view in a case, select the evidence device to run C4All against.
2. In the Component list, click Evidence Status.
3. In the Content pane, click **Run** next to Known Files for the device.
4. In the Hash Sets window, mark the checkbox for **C4All** and then click **OK**.



5. When the hashing process is complete, open the Media view for the selected evidence device. All media files (such as pictures, videos, and thumbnails) appear in the Content pane.
6. Choose one of these options to select all items in the view.
  - In the menu bar, click **Edit > Select All**.
  - Use the keyboard shortcut for your computer to select all.

Each selected item is in a yellow box.

7. Open the context menu and then click **Export > Export Data Model > C4All**.



8. Select a folder to save the exported files to, and then click **Export**.  
Inspector exports the images, videos, and thumbnails in the specified C4All format and creates all the index files that are normally associated with C4All.

The exported files are now ready to present to a trained child exploitation investigator.

## Semantics21

Semantics21 provides the LASERi suite of tools to examine images, animations, and videos. Once images are brought into the tool, they can be assigned to one of these categories,

- 0: Non-Pertinent
- 1: Child Abuse Material (CAM) Illegal
- 2: Child Exploitive (non-CAM) / Age Difficult
- 3: CGI / Animation - Child Exploitive
- 4: Comparison Images
- 5: Uncategorized

Inspector's integration with S21 allows users to complete these tasks.

- Export data in the S21 format.
- Import the data into an S21 tool.
- Use the S21 tool to set labels and assign category values.
- Connect Inspector to the S21 SQL Database (to see a list of S21 user databases).
- Run Known Files for S21.

### Export Images and Videos

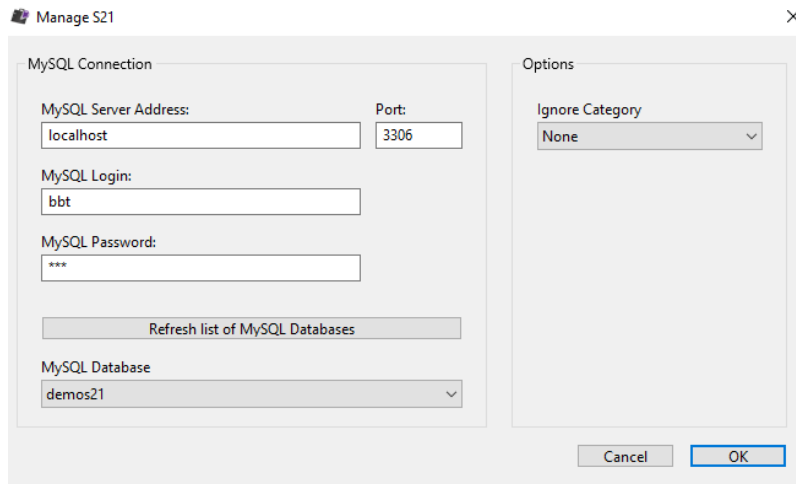
1. In Inspector, select the images and videos to export.
2. In the menu bar, click **Export > Export Data Model > S21**.  
A folder is created with a name based on the case name and the date and time the files were exported.

In the S21 export folder, movies are placed in an S21M folder and pictures are placed in an S21P folder. These folders contain an index file and subfolders containing the pictures and videos exported. The index files are named *S21P Index.xml* for pictures and *S21M Index.xml* for videos.

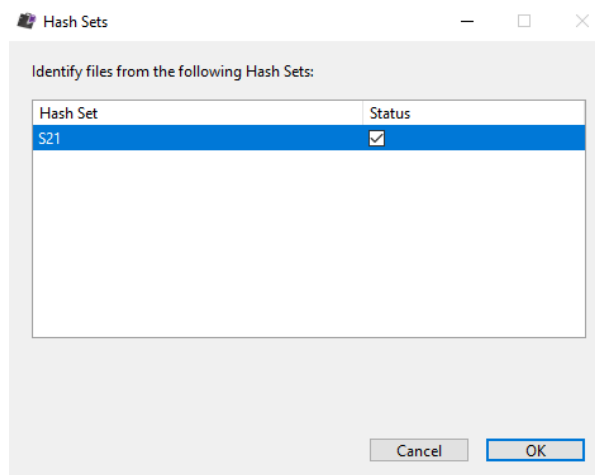
3. In the S21 tool, choose **S21P Index.xml** or **S21V Index.xml** to import the files into the appropriate LASERi tool. Once the files are imported, they can be categorized within the LASERi interface.

## Connect Inspector to the S21 SQL Database

1. In the menu bar, click **Manage > S21**.
2. Type your username and password.



3. In the Content pane, click **Evidence Status**.
4. In the Known Files column, click **Run** for the items you wish to run the S21 dataset on.



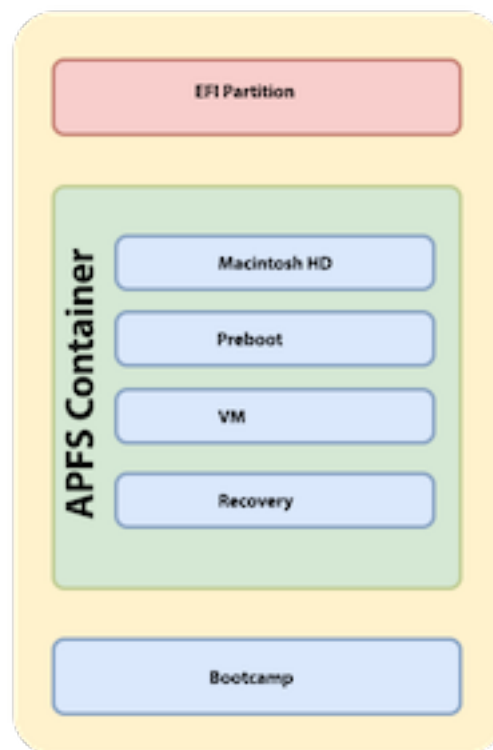
## File System Information

This chapter provides information about file systems that can be useful when you use Inspector.

- [Apple File System](#)
- [Artifact Items](#)

### Apple File System

The Apple File System (APFS) replaced HFS+ as the default file system beginning with macOS 10.13. APFS is much different than HFS+. APFS no longer defines a volume, rather it implements a container inside of which several volumes may be present. APFS was designed for solid state drives (SSDs) but can work with traditional drives as well.



APFS also uses Copy-On-Write, which means if you copy a file, the resulting copy will not duplicate the data on disk. Both inodes (original and copy) will point to the same original extents. Only when the copy is changed will new extents be allocated.

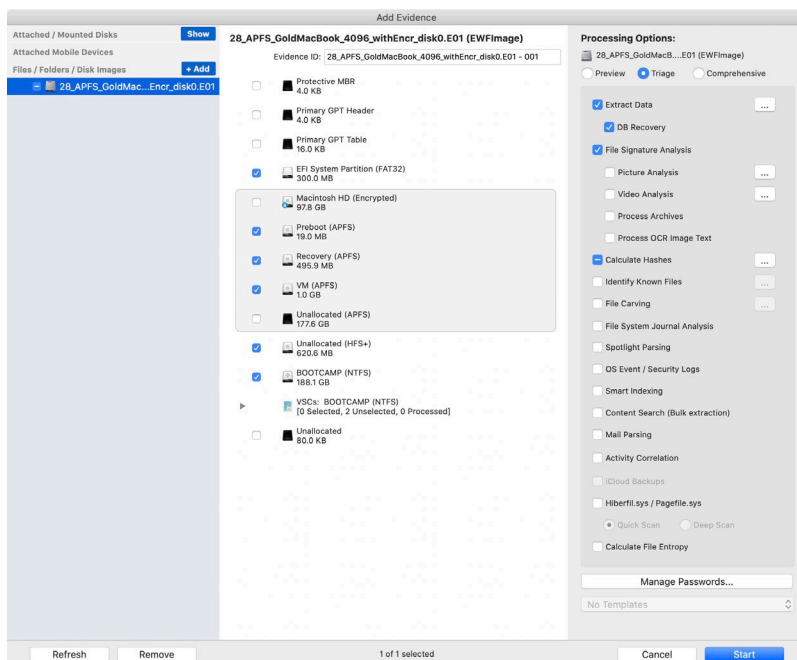
The APFS container by default does not have a limit on the size or location of the volumes within it. Unlike traditional partitions on disk where sectors are allocated for each volume before they can be used, APFS allows all volumes to share a common pool of extents and they all report having total free space as the same. This also means data from all volumes is interspersed and volumes are not contiguous. Space in the logical container pool can be used by one to more APFS volumes. APFS Volumes grow and shrink by allocating unused blocks from the logical container pool and retuning them when files are deleted, and space is freed. Each APFS

container only knows about the blocks used by its own active files, and unallocated space is managed within the logical container pool. Because APFS volumes within a container are not traditional partitions, these volumes in the container cannot be individually imaged.

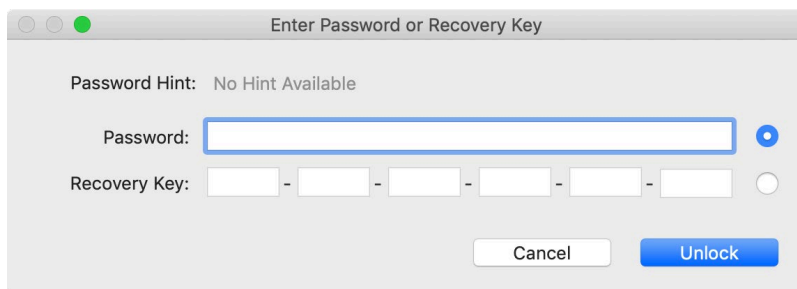
If you choose to run Digital Collector Live on the target system, keep in mind that on macOS 10.13.0 (and higher) while System Integrity Protection (SIP) is active, no user, even root can read the physical disk the system is currently booted from, the physical partition the system is currently booted from, nor the APFS container that holds the currently booted volume. This makes it impossible to image the physical disk.

## Adding APFS Evidence to Inspector

APFS is very different than any other file system so it will appear differently than what is typically seen. Specifically, the APFS container uses pooled storage, which is available to all volumes within it, including unallocated space. Inspector will present the APFS pooled container highlighted with a grey box around the pooled volumes. The other volumes will appear normally. If a volume is encrypted, a locked icon appears next to the volume and (Encrypted) appears after the volume size. Encrypted volumes are automatically deselected.

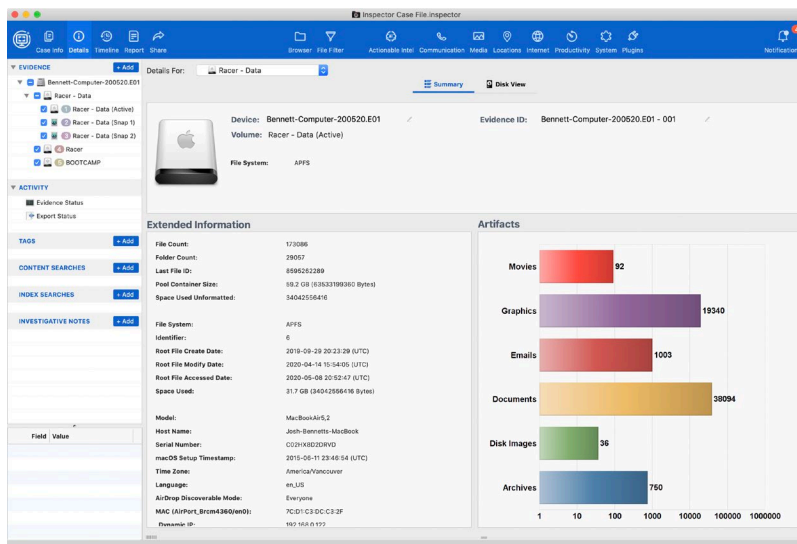


Mark the check box next to an encrypted volume within the APFS container. A password prompt appears where you can enter a password or a recovery key to unlock the volume.



Because APFS uses pooled storage, deleted files cannot be carved from volumes. You can only carve from pooled storage, which means File Carving must be chosen for the unallocated space in the APFS pool during initial evidence ingestion. Data can be carved from volumes not within pooled storage at any time during the analysis.

**Note:** It is not possible to carve unallocated from the pooled storage after the image is ingested unless the image is re-imported.



## APFS Snapshot Parsing

APFS was designed using Snapshots as a means for built in backup support. Snapshots leverage the copy-on-write property of APFS to provide “instant” backups of the entire state of an APFS volume. Snapshots can be mounted as read-only volumes that are exact copies of the file system state at the time they were taken. However, Inspector does not need to mount the Snapshots in order to process them. APFS snapshots are detected automatically and listed in the middle pane of the Add Evidence window.

Below each Snapshot entry is an indicator of the number of Snapshots selected, unselected, and processed. By default, none of the Snapshots are selected for processing.

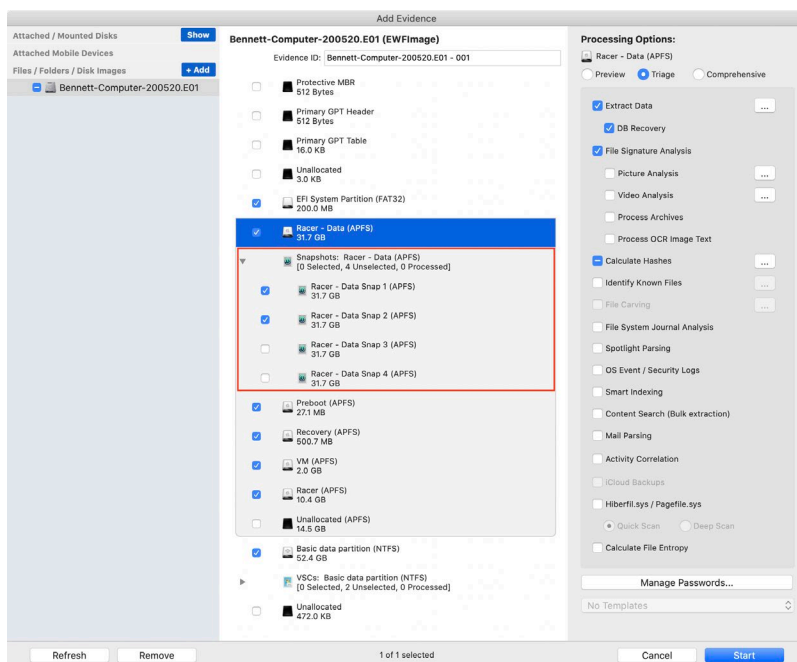
### Bennett-Computer-200520.E01 (EWFImage)

Evidence ID: Bennett-Computer-200520.E01 - 001

- ☐ Protective MBR  
512 Bytes
- ☐ Primary GPT Header  
512 Bytes
- ☐ Primary GPT Table  
16.0 KB
- ☐ Unallocated  
3.0 KB
- ☒ EFI System Partition (FAT32)  
200.0 MB
- ☒ Racer - Data (APFS)  
31.7 GB
- ☒ Snapshots: Racer - Data (APFS)  
[0 Selected, 4 Unselected, 0 Processed]
- ☒ Preboot (APFS)  
27.1 MB
- ☒ Recovery (APFS)  
500.7 MB
- ☒ VM (APFS)  
2.0 GB
- ☒ Racer (APFS)  
10.4 GB
- ☐ Unallocated (APFS)  
14.5 GB
- ☒ Basic data partition (NTFS)  
52.4 GB
- ☒ VSCs: Basic data partition (NTFS)  
[0 Selected, 2 Unselected, 0 Processed]
- ☐ Unallocated  
472.0 KB

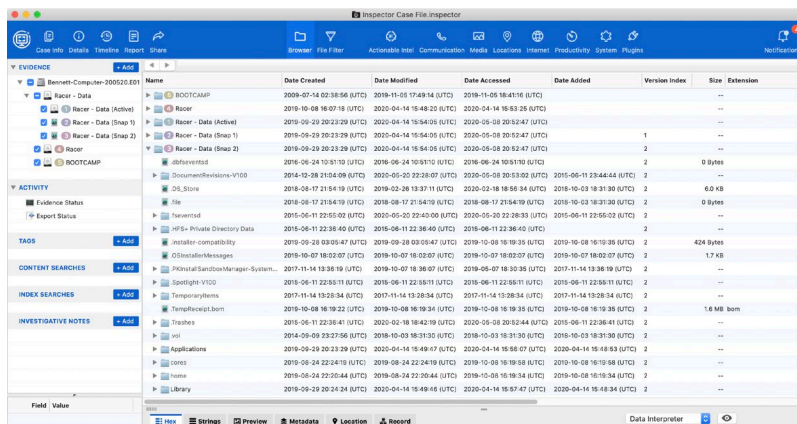


You can expand APFS Snapshots.



Once a snapshot is expanded, select specific snaps to process. As snaps are selected, the indicator for that snapshot is updated. Like all other volumes listed, different processing options can be set for each Snapshot. Processing all Snapshots take a longer time, and they do not have to be ingested during initial evidence processing.

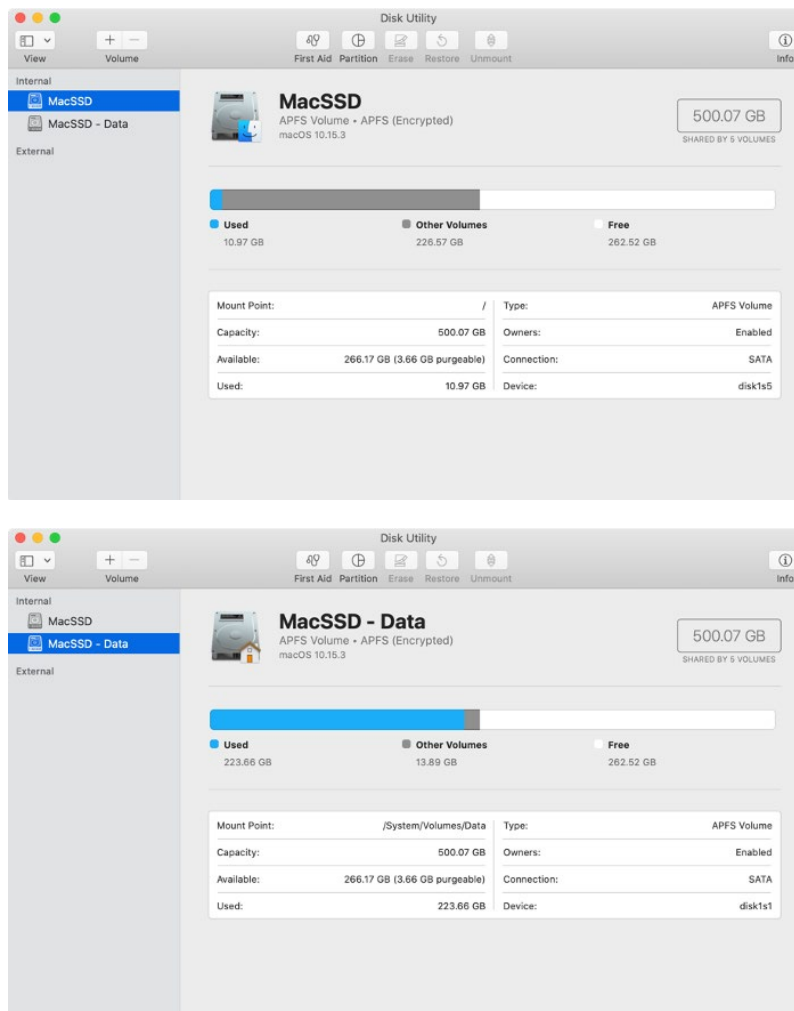
APFS Snapshots are automatically enabled if Time Machine is enabled, even if no backup disk is connected. Snapshots are created approximately every hour, before each Time Machine backup, and before certain system updates. The Snapshot lifetimes depend on a number of factors, but they are generally available for about 24 hours. Older snapshots may be deleted if the disk is low on space. We have found that devices with unsuccessful Time Machine backups tend to retain snapshots the longest.



## APFS on macOS 10.15

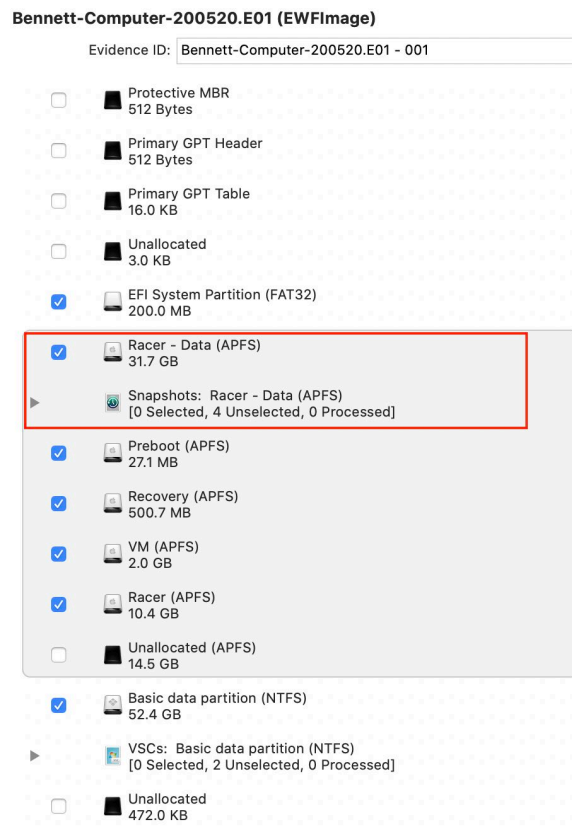
Increased system protection was added in macOS Catalina 10.15. The operating system runs in a read-only system volume, separate from other files. When a system is upgraded to Catalina, a second volume is created, and some files may move to a Relocated Items folder.

The boot volume was effectively split into two pieces. On the Desktop it appears as one volume, but looking at it via Disk Utility, it is readily apparent there are two volumes.



The volume name that appears on the Desktop appears in both volumes; the second volume has *- Data* appended to the volume name. For more information, see this topic provided by Apple: <https://support.apple.com/en-us/HT210650>.

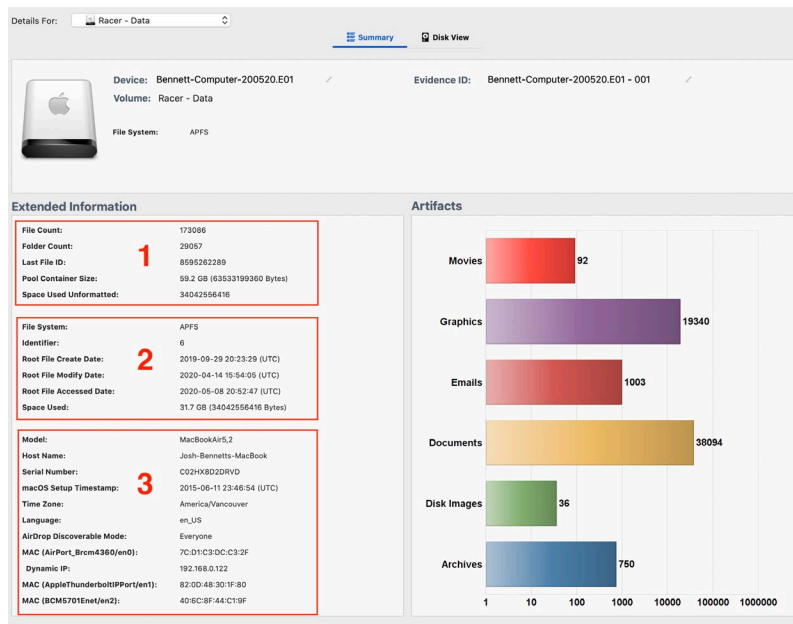
You can also see this structure when the volume is processed in Inspector. This can first be seen when ingesting evidence with a macOS 10.15.



This example shows a macOS computer with the volume name *Racer*. Evidence processing options can be different for the two volumes. User files and data are stored on the *<Volume Name> - Data* volume. When choosing processing options keep this in mind.

Once processed, the Details view shows different information for each portion of the volume. This is shown for the **<Volume Name> - Data** portion.

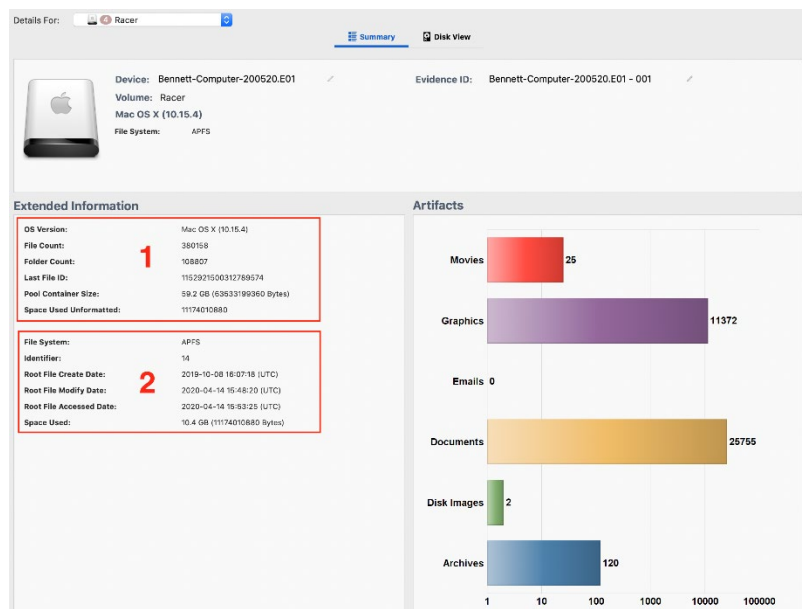
1. Information about data contained in this portion of the combined volume
2. Information pertaining to just the *<Volume Name> - Data* portion
3. Information about macOS system



This is shown on the Details view for **<Volume Name>**.

1. Information about the OS version and data contained in this portion of the combined volume
2. Information pertaining to just the *<Volume Name>* portion

During the examination, most of the user data will be found on *<Volume Name> - Data*. While there are pictures, videos, and other files on the *<Volume Name>* partition, they are related to applications and the operating system; they are not files created by the user.



## Artifact Items

These are the artifacts that Inspector can parse.

- [Spotlight Index](#)
- [NTFS Access Control Lists](#)
- [Cocoa Nanosecond Timestamp Format](#)

## Spotlight Index

Inspector can parse macOS Spotlight indexes. Spotlight is a system-wide search feature of macOS and the iOS operating systems. It allows users to quickly locate a wide variety of items on the computer, including documents, pictures, music, applications, and system preferences. Specific words in documents and in web pages in a web browser's history or bookmarks can be searched. It also allows users to narrow down searches with creation dates, modification dates, sizes, types, and other attributes.

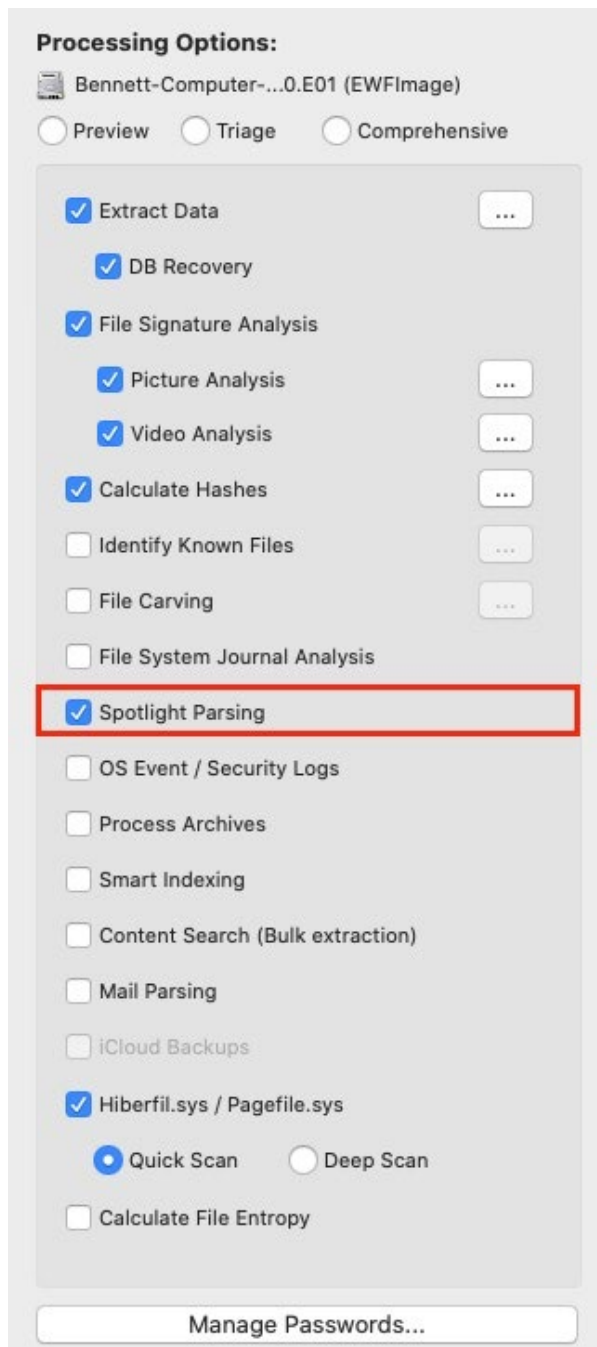
You can choose to run the Spotlight Parsing option in the Add Evidence window or in the Evidence Status pane.

Spotlight data is parsed into multiple locations in Inspector.

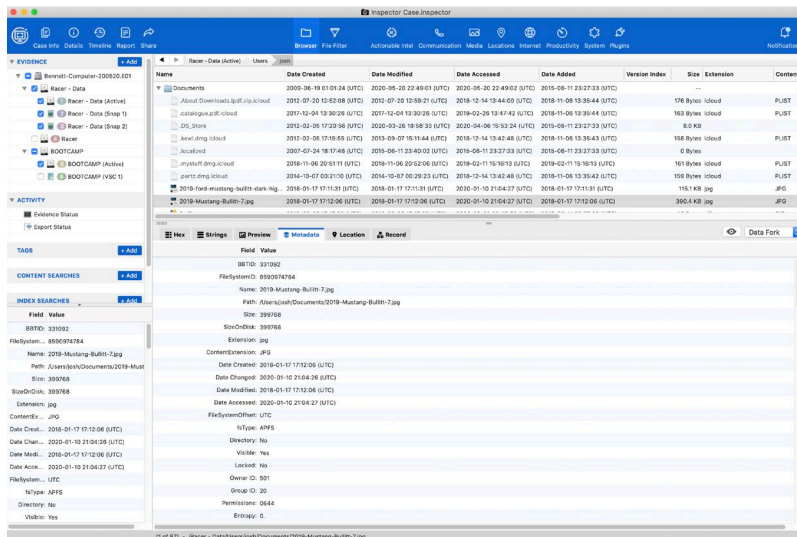
- Spotlight sub-view in the System view
- In the Actionable Intel view
  - Spotlight Search Shortcuts in the Search sub-view
  - AirDrop artifacts in the Downloads sub-view
  - recently accessed files in the File Knowledge sub-view

For more information, see these topics.

- [System View](#)
- [Actionable Intel View](#)



The Spotlight index items can also be located in the Metadata sub-view of the File Content view for any item in a macOS or iOS volume. All of the items will exist under the Spotlight heading within the metadata. There is a lot of information within this heading, some of which exists in the file itself as well as within the file's own metadata. However, there can also be much more useful information, such as dates and times.



In addition to the Metadata sub-view for Spotlight indexes, you can filter on these pieces of information within the Filter view.

## NTFS Access Control Lists

File system permissions in NTFS are controlled with Access Control Lists (ACL), which are ordered lists of ACEs (Access Control Entries). Each user logged onto the system holds an access token with security information for that logon session. The system creates an access token when the user logs on. Every process executed on behalf of the user has a copy of the access token. The token identifies the user, the user's groups, and the user's privileges. A token also contains a logon SID (Security Identifier) that identifies the current logon session.

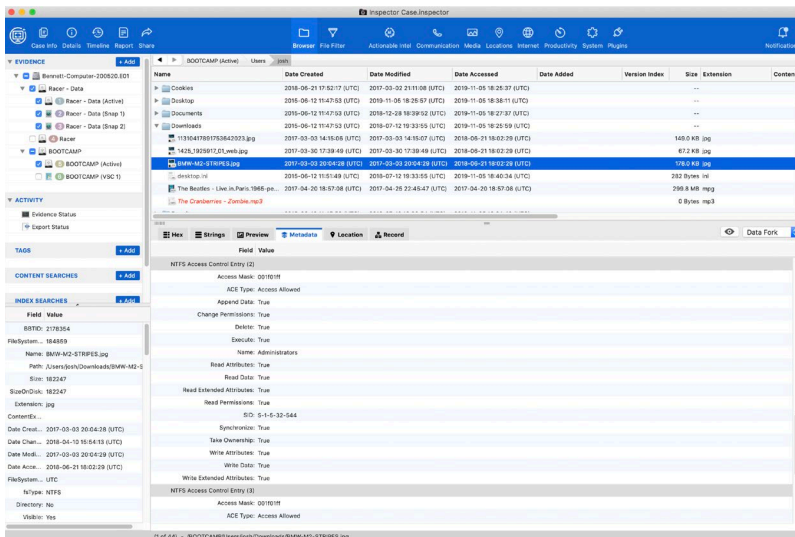
Each ACE in an NTFS ACL contains these items.

- A SID (Security Identifier) that identifies a particular user or group
- An access mask that specifies access rights
- A set of bit flags that determine whether or not child objects can inherit the ACE
- A flag that indicates the type of ACE

ACEs are fundamentally alike. What sets them apart is the degree of control they offer over inheritance and object access. There are two types of ACEs.

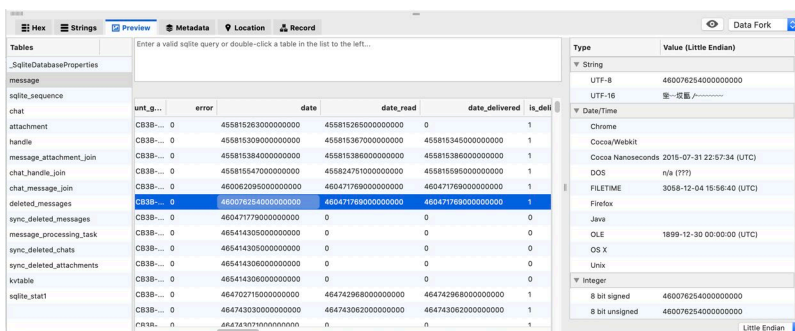
- Generic type that are attached to all securable objects
- Object-specific type that can occur only in ACLs for Active Directory objects

In the Metadata sub-view, you can see the ACE entries for each type that exists for the selected file.



## Cocoa Nanosecond Timestamp Format

From time to time, Apple changes storage formats for certain things. The Cocoa format for timestamps was introduced in iOS 11 and macOS 10.13. Instead of the previous 9 digits, Cocoa timestamps are 18 digits for some date columns. Inspector supports these longer nanosecond timestamps when they are encountered.



## Troubleshooting

This chapter provides these topics about troubleshooting for Inspector.

- [The Debug Console](#)
- [Other Issues](#)

### The Debug Console

Inspector may on rare occasion “hang” or unexpectedly quit. If this happens, relaunch Inspector, and then get the Dongle ID from the About Inspector window.

- On Mac computers, in the menu bar, click **Inspector > About Inspector**.
- On Windows computers, in the menu bar, click **Help > About Inspector**.

When you contact Technical Support, you will need the Dongle ID. For more information, see [Getting Support](#).

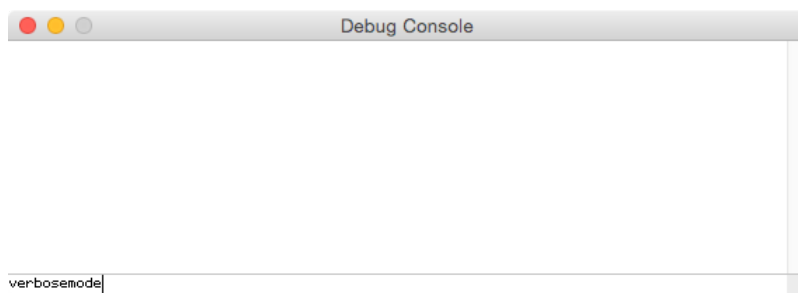
The Debug Console also opens in the lower left corner of the screen. You may open the Debug Console before you open a case to see more information that may be of interest.

There are several commands for the Debug Console that may yield additional troubleshooting information. Before you run and attempt to troubleshoot an Inspector process, you must enable verbose mode.

**Note:** Inspector runs much slower than usual when verbose mode is on.

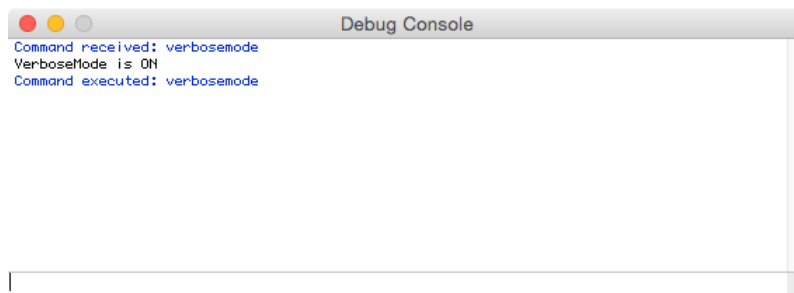
### Enable Verbose Mode

- In the lower left corner of the Debug Console, type **verbosemode**.





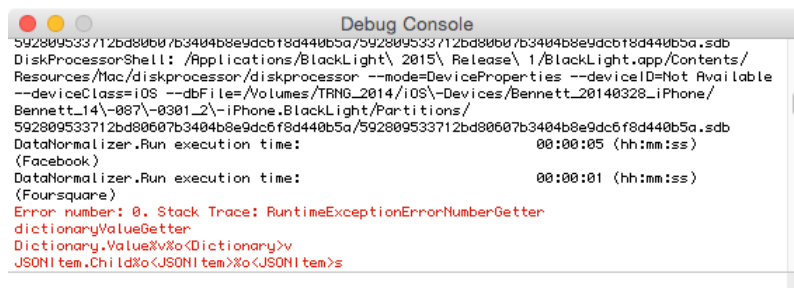
The Debug Console window shows additional information.



These are additional Debug Console commands.

| Command     | Description                                                                      |
|-------------|----------------------------------------------------------------------------------|
| systemlog   | Save the debug log to the console or system log                                  |
| logfile     | Save the debug log to a file named <i>Inspector Debug Log.txt</i> on the Desktop |
| verbosemode | Enable verbose mode debugging                                                    |
| watchmemory | Display Inspector objects' memory usage in real time                             |
| memused     | Show how much memory is currently in use                                         |
| objects     | Display all the objects Inspector is using                                       |
| objectcount | Show the number of objects Inspector is using                                    |

Errors appear in **red font in the Debug Console**. For example, the text **DiskProcessor is Restarting** may appear. While this is technically an error, there is no problem. *DiskProcessor* restarts itself in the event of an error, and this information is shown in the Debug Console.

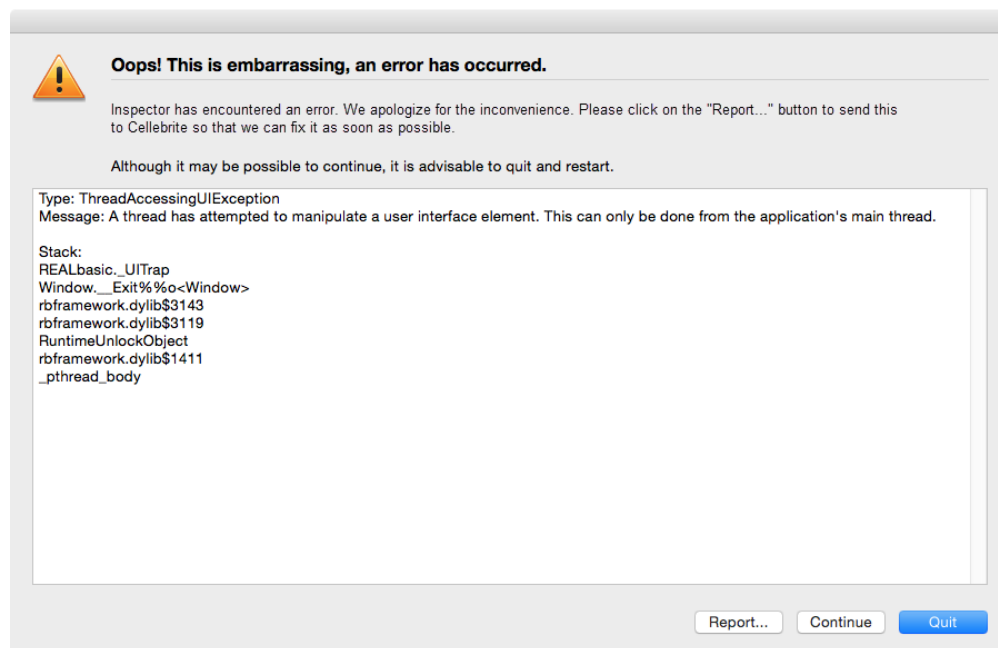


## Other Issues

Inspector may encounter files that cause the application to "hang" or close unexpectedly. Logs created as a result of these responses are very useful during the troubleshooting process. If possible, please have these logs available when you contact Cellebrite Technical Support. Unfortunately, logs are often not created, and determining the exact cause is difficult.

## Exception Errors

When an exception error occurs, Inspector shows an error alert.



If this happens, click **Report**. This sends the error report to Cellebrite so we can attempt to fix the problem as soon as possible.

If you would like our support team to contact you by email for assistance and follow up, type your contact information in the **Name and/or Email** field in the Problem Report window. In the **Comments** field, please include any information about what tasks were being performed when the error occurred or provide steps so that we can attempt to recreate the error during the troubleshooting process.

## Database Errors

The deleted SQLite record recovery process can cause a database error, more often on a Windows analysis computer than on a Mac. You can remedy this issue on the Options tab in the Preferences window by unmarking the checkbox for **Recover Deleted SQLite Records**. For more information, see [Inspector Preferences or Options](#)

This prevents Inspector from attempting to recover deleted SQLite records.

If disabling this option does not remedy the issue, open the Debug Console, issue the verbose mode command, and repeat the action undertaken prior to the crash.

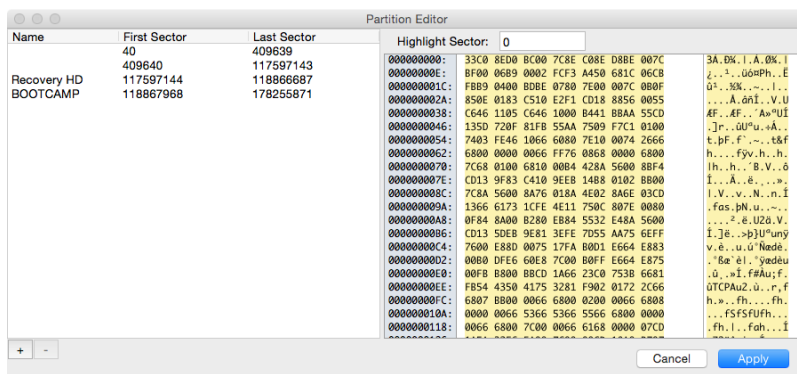
Searching container files such as .tar and .zip files can also cause issues. If this happens in a case when deep search has been enabled, you can disable deep search to prevent Inspector from searching inside a container or compound files. However, you will have to manually extract and examine container or compound file types.

## Locating Partitions

Sometimes Inspector may not automatically locate a disk image, disk image partition, or the correct disk image partition. This problem often occurs if the GUID, Apple partition map, or the Master Boot Record has been wiped, though the partitions remain present. You can remedy this by either extracting the partitions and then adding the extracted partitions back to the case as separate devices, or by adding a new partition to the image file.

1. At the top of the Component list, click **Add**.
2. Navigate to the disk image and click **Open**.
3. In the Add Evidence window, open the context menu from the image file name and click **Edit Partitions**.

The Partition Editor window appears with each volume's start and end sector information.



4. In the bottom left corner of the Partition Editor window click **+** (add).  
A new partition entry appears.
5. Under the name column, type the new partition name.
6. Under the **First Sector** and **Last Sector** columns, type the partition's start sector number and end sector number, respectively.
7. Click **Apply**.

Inspector recognizes the new partition, displays it in the Evidence section of the Component list, and makes partition data available for analysis.

If a problem with Inspector persists, please contact Cellebrite Technical Support. For more information, see [Getting Support](#).

## Appendix 1 - iTunes Precautions

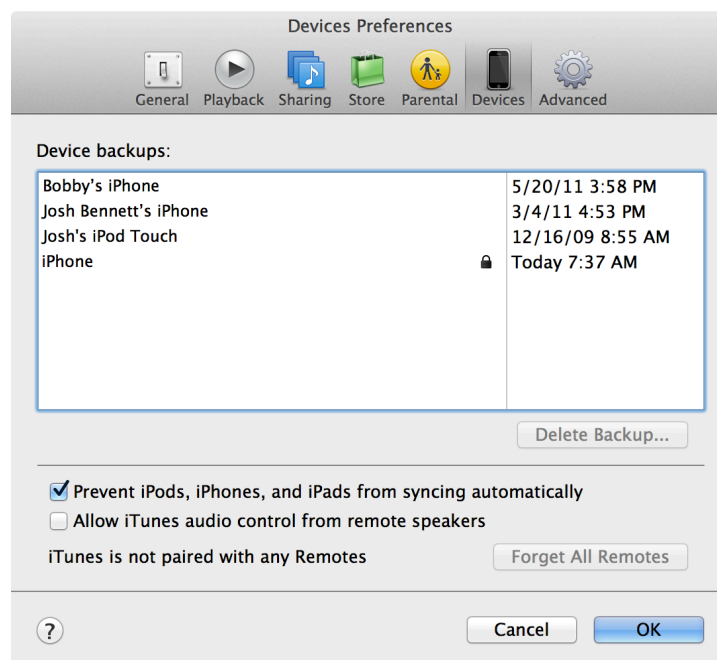
All of these precautionary procedures are highly recommended for the analyst to remain in full control of the computer. If any application auto-launches while a device is attached, the application may cause adverse effects to evidence.

To prevent inadvertent data writes to an evidentiary iOS device, you must prevent iTunes from launching when an iOS device is attached to an analysis machine. The methods for doing so differ depending on whether the iTunes application has been previously launched under the current user account on the analysis computer.

If iTunes has been launched under the current user account on the analysis computer, before you attach an iPhone to the analysis computer, you must disable the iTunesHelper application. This application launches iTunes automatically when an iOS device is attached to the computer. Disabling this application prevents iTunes from launching.

### Disable iTunes on a Mac Computer

1. Launch iTunes.
2. At the top of the screen on the menu bar, click **iTunes > Preferences**.
3. Click **Devices**.

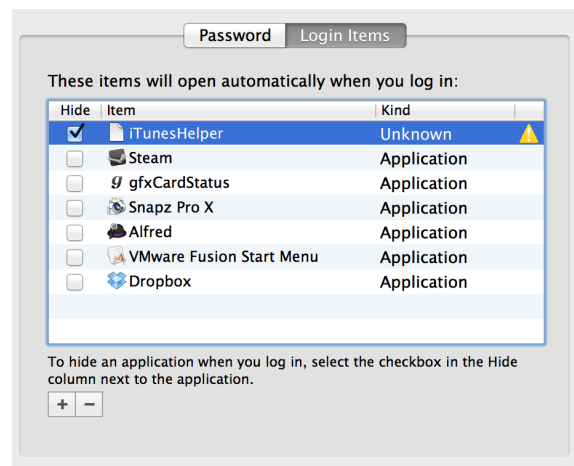


4. Mark the checkbox for Prevent iPods, iPhones and iPads from syncing automatically, and then click **OK**.
5. On the menu bar, click **iTunes > Quit iTunes**.

Next, disable the iTunesHelper application to prevent the iTunesHelper application from automatically launching during login.

## Permanently Disable iTunesHelper on a Mac Computer

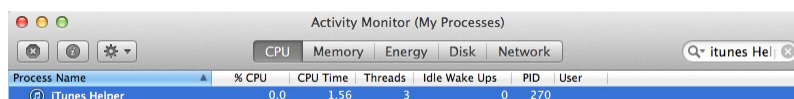
1. Click anywhere on the Desktop.
2. On the menu bar, click **Apple > System Preferences**.
3. Click **Users & Groups**. (On versions of OS X earlier than Lion, click **Accounts**.)
4. On the preferences window, click **Login Items**.
5. In the Hide column, mark the checkbox for **iTunesHelper**.



6. Below the list, click **- (remove)**.  
The iTunesHelper application is removed from automatic login items list.

## Temporarily Disable iTunesHelper on a Mac Computer

1. Launch the Activity Monitor application, which is located here:  
*/Applications/Utilities/Activity Monitor*.
2. In the Activity Monitor menu, click **View > My Processes** (if it is not already selected).
3. In the **Filter** field, type **iTunes Helper**.  
The iTunes Helper application process is isolated.



4. Select the iTunes Helper application.
5. In the top left corner of the Activity Monitor window, click **Quit Process** (the stop sign with an X in it) and then click **Quit**.

The iTunesHelper application is disabled, and iTunes will no longer automatically launch when an iOS device is attached to the analysis computer.

You can reactivate iTunesHelper. Either locate the application and manually launch it, or add it back to the list of login items and then log out and back in. The iTunesHelper application process appears in the Activity Monitor process list when it is active. For recent versions of iTunes on a Mac, open this folder in Finder to locate the iTunesHelper application:  
*/Applications/iTunes/Contents/MacOS/*

## Disable Auto-Launch of Camera-Related Applications on Mac Computers

OS X features a running daemon named *PTPCamera*. This daemon checks for the connection of a camera device, and most iOS devices include camera functionality. In the default configuration of OS X, the Image Capture application launches when a camera device is connected to the system. Image Capture has an option to stop auto-launch when a specific device is connected, but it does not offer a way to control the connection of new camera devices.

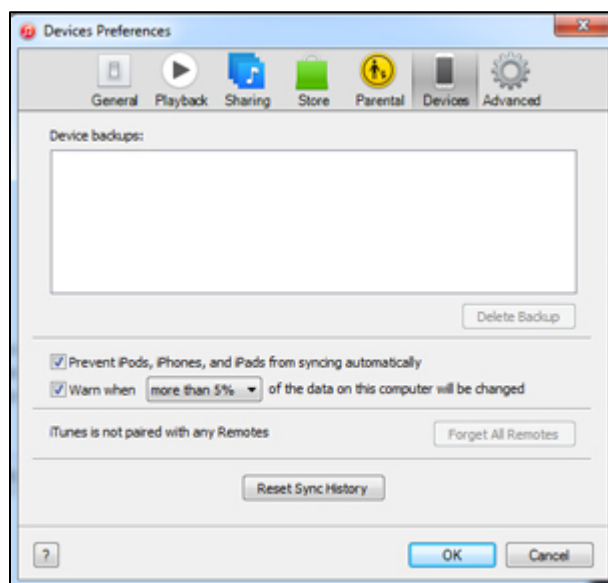
iPhoto, however, offers the ability to control auto-launch for all camera devices. In fact, with iPhoto, the user can select a preference to never auto-launch any camera-related application, including Image Capture, when camera devices are attached.

1. To set this preference, open the iPhoto application and click **iPhoto > Preferences**.  
The iPhoto General preferences window appears.
2. In the **Connecting camera opens field**, select **No application**.

A specific key in the user's *Library/Preferences* folder is set, stopping applications related to the camera function of any camera device.

## Disable iTunes on a Windows 10 Computer

1. After launching iTunes, in the menu bar, click **iTunes > Preferences**.
2. On the General Preferences window, click **Devices**.
3. Mark this checkbox: **Prevent iPods, iPhones and iPads from syncing automatically**.



4. Disable the iTunesHelper application to prevent it from automatically launching during login.
  - a. Open the Task Manager, and on the Startup tab, disable iTunesHelper.
  - b. On the Processes tab, right-click on *iTunesHelper.exe*, and then click **End task**.

## Disabling Windows AutoPlay features

AutoPlay is active on Windows 10 by default. It does not appear to automate anything with iOS devices that are attached, but it is best practice to disable it.

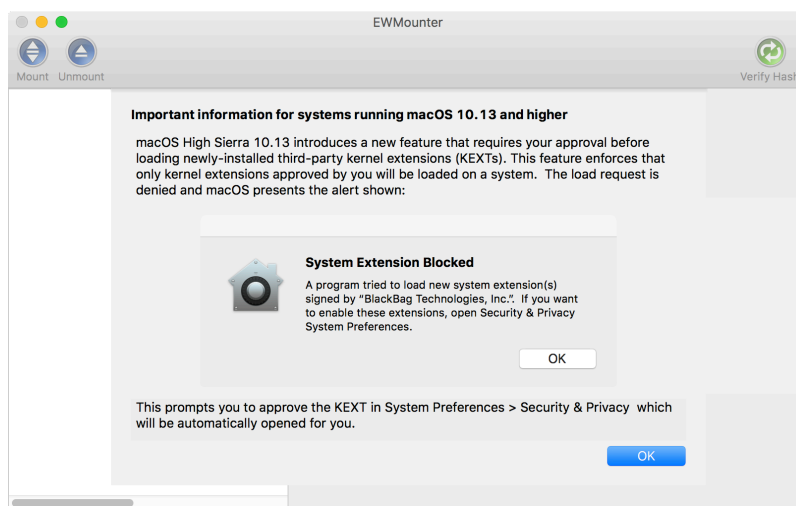
For more information, see Disabling Windows AutoPlay in [System Settings on Windows 10 Computers](#).

## Appendix 2 - EWMounter

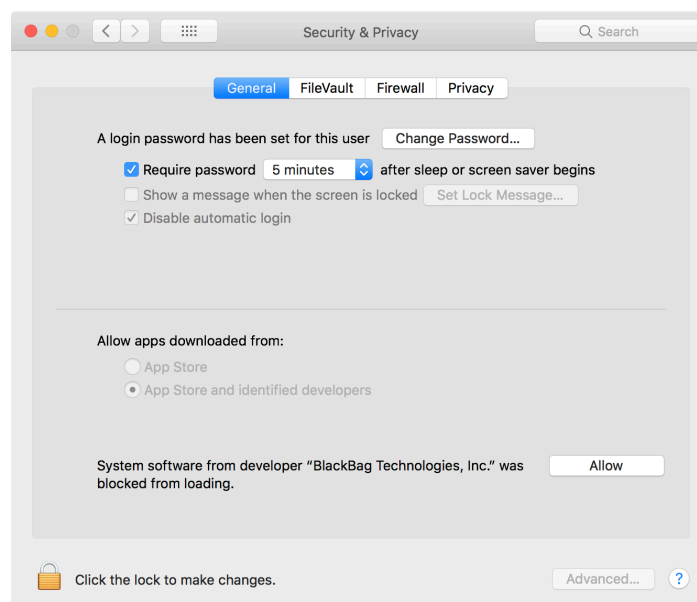
Inspector ships with a separate E01 forensic image mounting application that allows examiners to mount E01 image files on a Mac computer. You can save a lot of time by mounting a forensic image as a connected device and browsing the directory structure before acquiring data from the image file. Mounting an E01 forensic image file is also helpful in the course of a forensic examination of Mac computers, because you may be able to open non-native application files that cannot be opened from within Inspector.

Inspector supports EWMounter on macOS up to 10.15.7.

On Mac computers running macOS 10.13 and higher, when EWMounter is run for the first time, this warning appears.



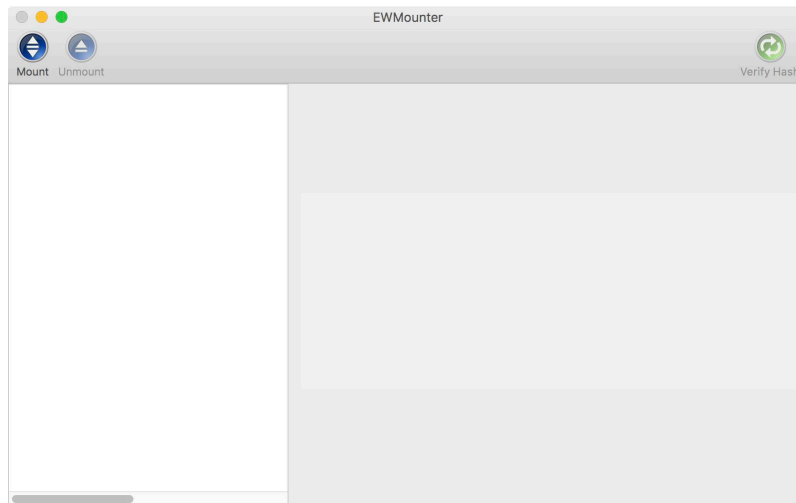
Click **OK**. The Security & Privacy tab in the System Preferences window appears. Click **Allow**.





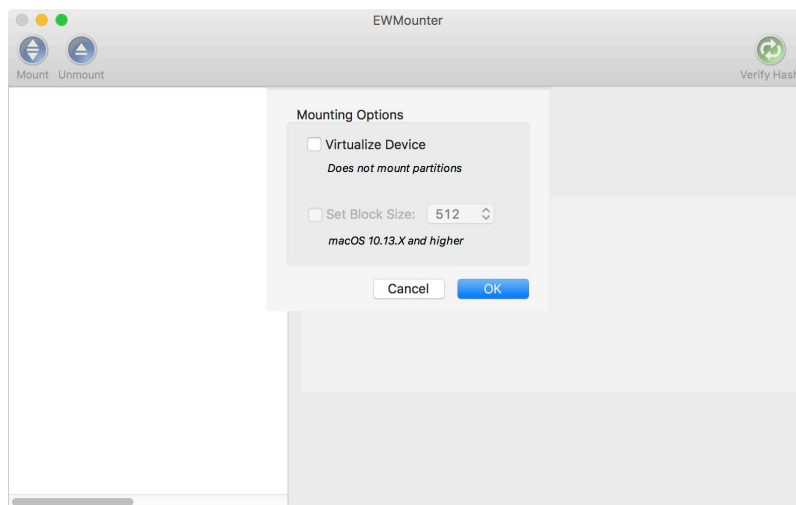
**Note:** You must run EWMounter from an administrator account. It cannot be run from a standard user account.

To launch the EWMounter application, double-click the application icon in the `/Applications/Inspector` folder. The EWMounter application window appears.



## Mounting Options

To mount an E01 image file click **Mount**. Navigate to the E01 file and click **Open**. The Mounting Options window appears.



To mount the file (and partitions) normally, unmark the **Virtualize Device** checkbox. Under most circumstances, the Virtualize Device checkbox should not be marked.

If the E01 file is damaged, you can create a file system entry without mounting the E01 file by marking the **Virtualize Device** checkbox. You can mount the E01 file as a virtualized device to create a file system entry, and then run the 'dd' utility (convert and copy), or other disk recovery tools.

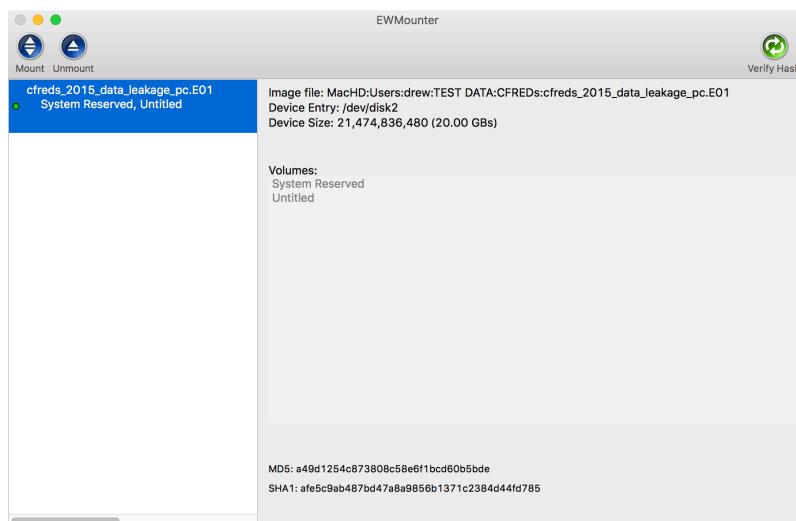
On macOS 10.13 and higher, the Set Block Size option is available. This lets you set different block sizes based on the type of image. Advanced Format hard drives ship with 4k sector sizes, which do not mount properly with a 512 (default) block size. To properly mount such an image, mark the **Set Block Size** checkbox and choose a size, then click **OK**. Available sizes are 512, 4096 and 8192.

A block size of 4096 should be selected for images of a 2015 MacBook, 2015 MacBook Air, and any Mac model shipped with an SSD in 2016 and later.

EWMounter opens and mounts the E01 image with the options you set.

**Note:** Additional non-E01 files may appear as selectable in the navigation window. But when selected, they fail to launch because EWMounter only opens E01 image files.

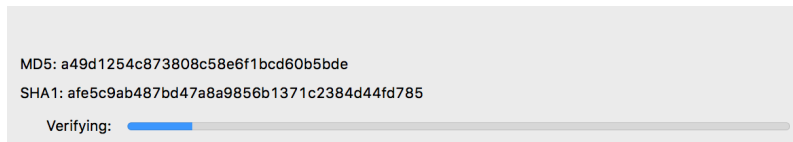
On the left side of the EWMounter window, the mounted E01 file shows a green dot to the left of the file name. Select the E01 image file name. On the right side of the EWMounter window under Volumes, the E01 image file partitions display along with the image file's MD5 and SHA1 hash values.



Not all E01 files have a SHA1 hash value. If an E01 image file does not have a SHA1 hash value, only the MD5 hash value appears.

## Verifying MD5 and SHA1 Hash Values

To verify the E01 image MD5 and SHA1 hash values in EWMounter, click **Verify Hash**.

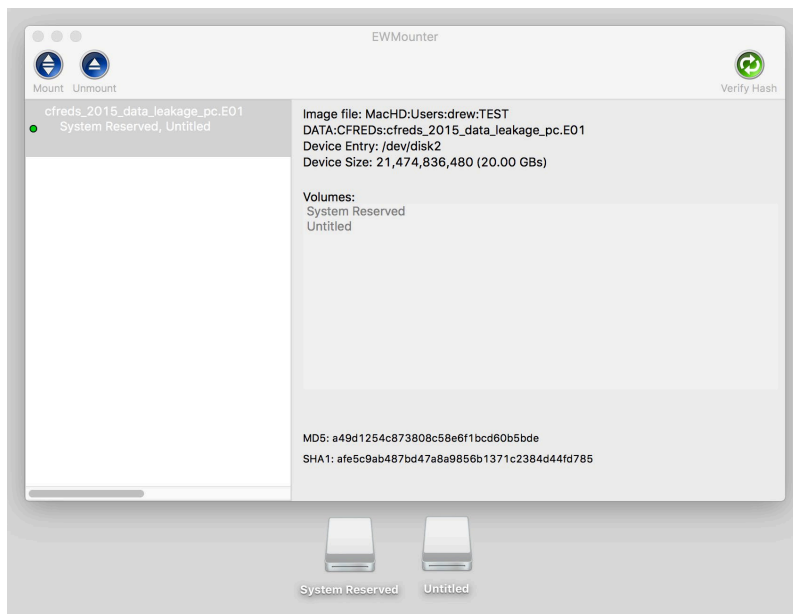


If the hash verification succeeds, (Verified) appears. If the hash verification fails, (Failed) appears.



**Note:** If a hash verification fails, the E01 image file may not be identical to the source device. This warrants further attention.

Mounted E01 image files also mount as part of the file system on the analysis computer and are visible as a mounted device on the Desktop and in a Finder window. This example shows mounted E01 image file partitions in the EWMounter window as they appear mounted on the Desktop.

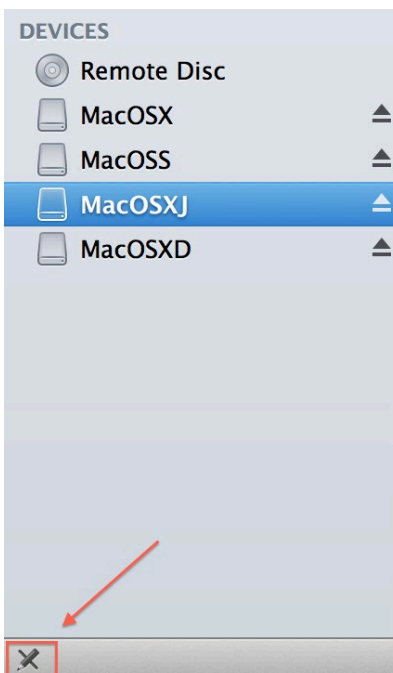


## Previewing a Mounted E01 Image File

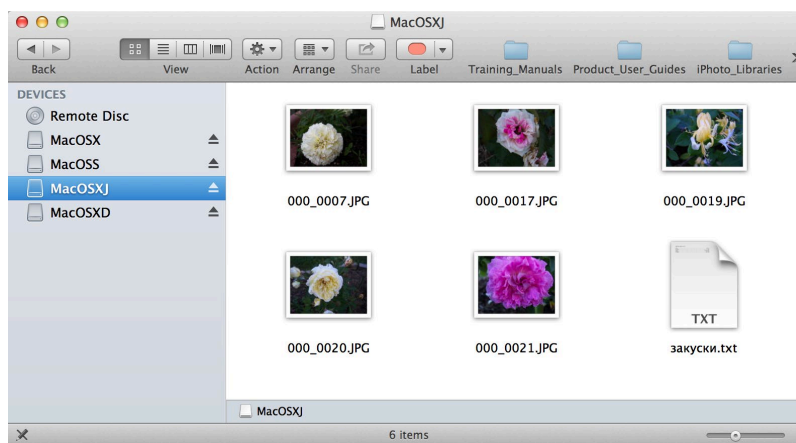
You can preview a mounted E01 Image File in Finder and in Inspector.

### Previewing in Finder

A mounted volume may be opened in the Finder and the contents previewed as if the volume was physically attached to the analysis system. Volumes are mounted with read-only permissions and are therefore write-protected, as indicated in the lower left corner of the window that displays a small pencil symbol with a line through it.



This example shows the contents of a mounted volume in a Finder window, and confirms the volume is read-only.



## Previewing in Inspector

To preview the contents of an E01 file in Inspector, mount the E01 file using EWMounter. After the E01 file is mounted, follow the same process as for adding any attached device to a case in Inspector. For more information, see [Adding Evidence to a Case](#).

In the Add Evidence window, to the left of the mounted E01 disk image or partitions, mark the checkboxes. In the right pane of the Add Evidence window, select the options for ingestion and processing, and then click **Start** to begin adding the attached E01 to the case.

**Note:** This preview technique is intended as a triage tool. If data of interest is discovered during the triage process, you may remove the attached E01 file preview from the Inspector case and formally import the E01 image file contents into the case. To do so, in the Component list, select the attached E01 image, open the context menu, and select **Remove Evidence Item**. Unmount the image in EWMounter. In the Component list to the right of Evidence, click **Add**. The Add Evidence window appears. Select the E01 file, choose processing options, and then click **Start**. Inspector imports the E01 image file into the Inspector case.

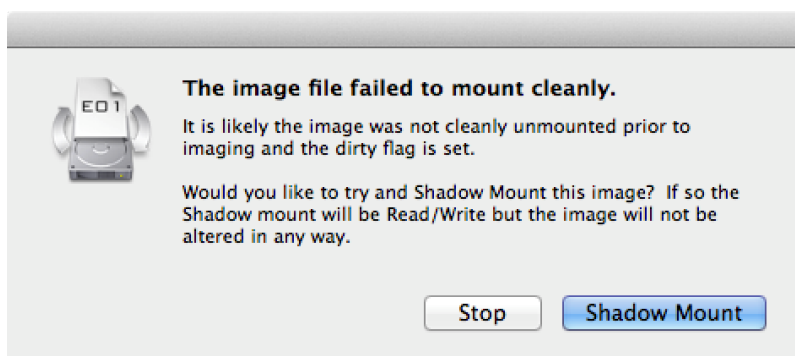
For more information, see [Managing Case Evidence](#).

## Shadow Mounting an E01 Image File

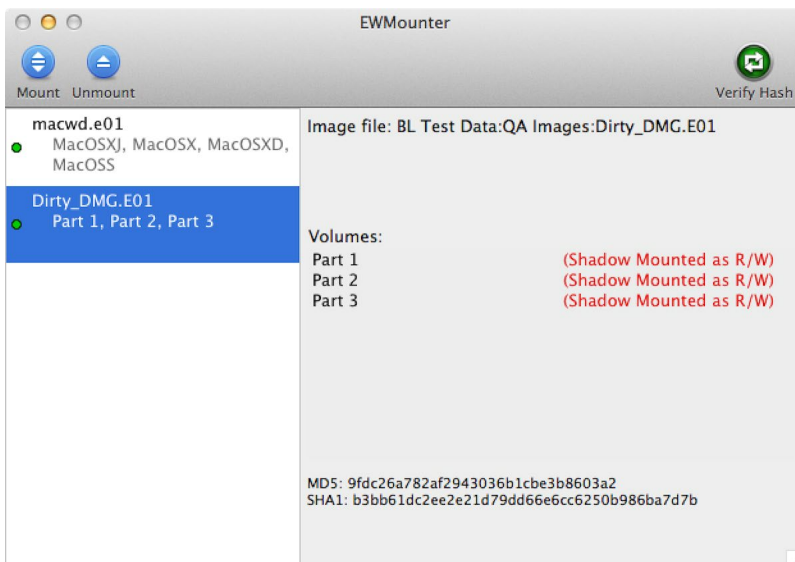
E01 image files sometimes contain partitions that do not mount cleanly. These partitions are marked as “dirty” in the file system (the ‘dirty bit’ is ‘flipped’). A File System Consistency Check (FSCK) must be run to successfully mount the file.

Running an FSCK check normally causes writes to be written to a volume. EWMounter handles this issue automatically by shadow mounting the volumes and running the FSCK check on the shadow volume.

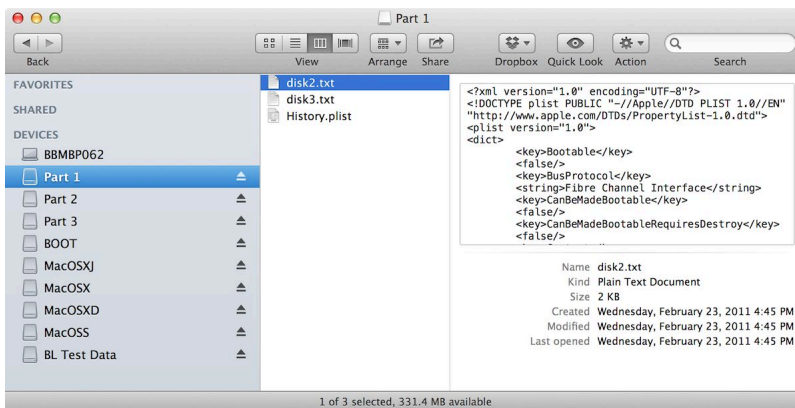
Shadow mounting an E01 image file does not affect the original E01 forensic image in any way. No writes are made to the E01 image, so no changes are made to the forensically sound image. However, the shadow file does have Read-Write permissions, so changes can be made to it during the FSCK check.



Shadow mounted volumes display with a **Shadow Mounted as R/W** label in red text to the right of the volume name.



The screenshot below shows two files (*disk2.txt* and *disk3.txt*) on a shadow mounted volume as seen in Finder. There is no pencil icon (read-only) symbol in the lower left corner of the Finder window.

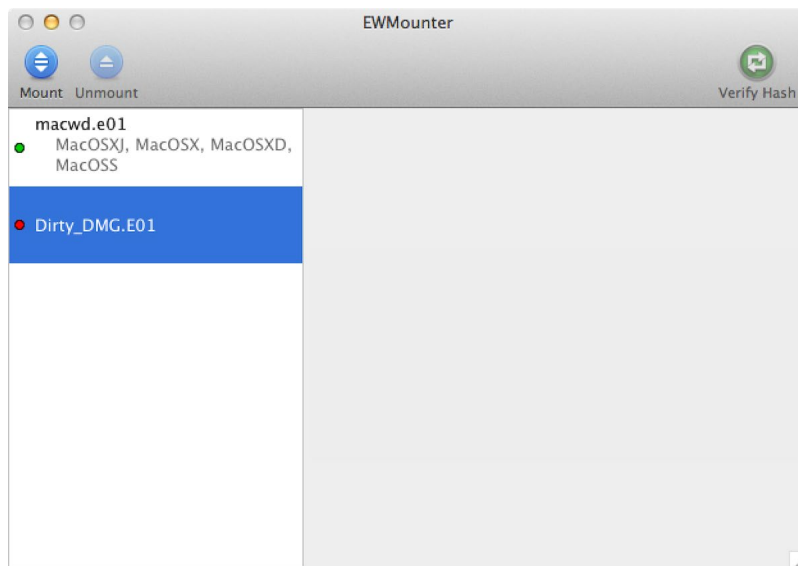


Because the shadow file has read-write privileges, some file information, such as dates and times, may be inaccurate. Time stamps may represent the time the examiner shadow mounted the image and the time the FSCK check occurred, and not the original image file timestamps. An examiner can add or delete files to and from a mounted shadow file.

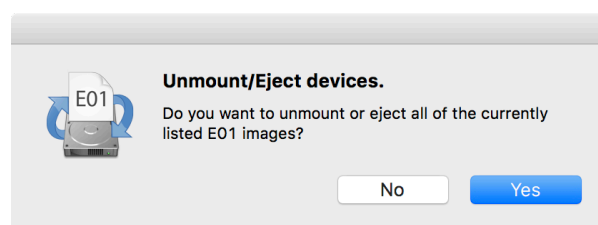
## Unmounting an E01 Image File

When the E01 volumes are no longer needed, you can unmount the volumes in the EWMounter application

Select the E01 image file. In the top left corner of the window, click **Unmount**. On the left side of the EWMounter application window, the mounted E01 file displays with a red dot to the left of the file name, indicating the image file is unmounted.



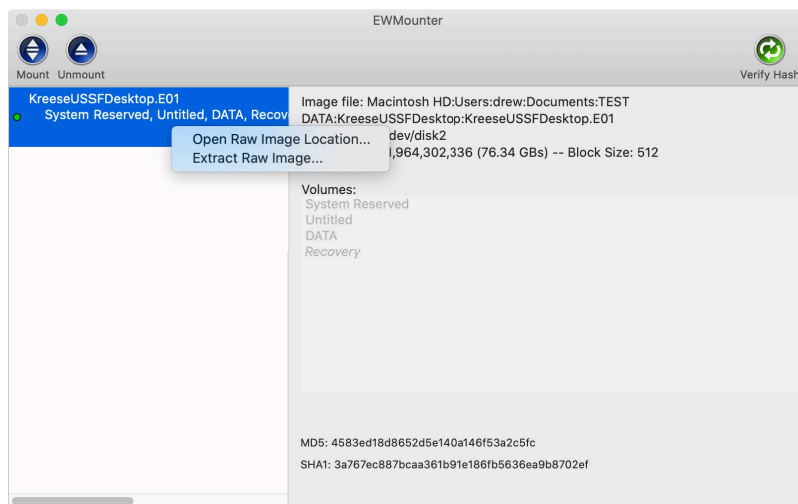
If the volume does not fully unmount, check to see if the volume is still in use. Quit any running applications associated with the image and unmount the volume from the Finder application. If the EWMounter application is quit while still having mounted filesystems a warning appears, asking if those devices should be unmounted or ejected.



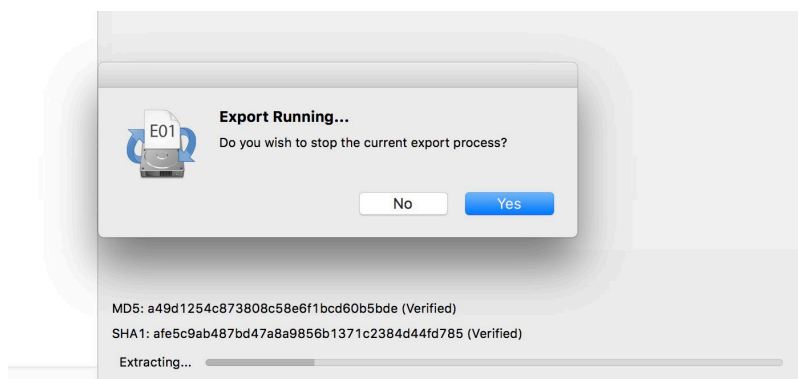
## Extracting RAW images from EWMounter

You can extract the raw image from within the attached E01 file.

On the left side of the EWMounter window, select the attached E01 image with a green dot and open the context menu, then click **Extract Raw Image**. The raw disk image will be extracted to the selected location.



**Note:** Only a single image can be exported at a time. If a second image export is attempted, EWMounter shows a warning, and you must choose to continue or stop the current process and remove the exported raw image file. The same warning appears if an E01 is unmounted during an export process.





## Appendix 3 - Inspector License Server Configuration

The Inspector License Server allows labs with multiple forensic analysis computers to authorize Inspector over a Local Area Network (LAN). Multiple Inspector dongles (one for each analysis computer) are not needed with the Inspector License Server in place.

Follow the instructions included in the software activation email to register and license the Inspector License Server dongle. Connect the Inspector License Server dongle to the designated computer and install the Inspector License Server application.

Click the **Inspector License Server** icon to launch the Inspector License Server.



The Inspector License Server shows all current product licenses contained on the License Server dongle. The IP address and default License Server port, 6672, appears at the bottom of the window.

| Cellebrite Inspector License Server |       |      |           |
|-------------------------------------|-------|------|-----------|
| Product                             | Total | Used | Available |
| BlackLight                          | 1     | 0    | 1         |
| Inspector                           | 5     | 0    | 5         |
| Address: 192.168.1.148:6672         |       |      |           |

To change the default License Server port, create a text file named *Inspector License Server Settings.txt* and save it in the same folder as the Inspector License Server application. In that text file, type **Port = NNNN**, where NNNN is the appropriate port number.

To configure an Inspector forensic analysis client computer, connect the computer to the same network segment as the computer running the Inspector License Server. Create a text file to tell Inspector to look for the License Server if a local USB dongle is not present.

1. Create the following file in the current examiner's home directory:
  - macOS: `~/Library/Application Support/Cellebrite/Inspector/Network Dongle.txt`
  - Windows 10: `~\AppData\Roaming\Cellebrite\Inspector\Network Dongle.txt`
2. Add a line with the server IP address and port (located at the bottom of the License Server window) in this format: **Server = 172.17.2.20:6672**

This tells Inspector that if an Inspector dongle is not connected to the computer to look for the License Server at 172.17.2.20 over port 6672.

**Note:** For the Cellebrite folder to exist, Inspector needs to be launched at least one time on the client computer. The file name *Network Dongle.txt* is case-sensitive.

When a networked forensic analysis client authorizes Inspector via the License Server, the License Server subtracts one license from the total number of available licenses on the License Server dongle.

When all available Inspector License Server licenses are in use, additional instances of Inspector fail to initialize. Additional licenses must be purchased and installed on the License Server dongle, or an examiner must release the license on a currently authorized client computer by exiting Inspector or by shutting down the currently authorized computer.

Once a license becomes available, either through purchase or when a client computer releases an authorization, another forensic analysis computer can run Inspector.